Extended modules over skew PBW extensions

William Alfredo Fajardo Cardenas

Universidad Nacional de Colombia
Facultad de Ciencias, Departamento de Matemáticas
Bogotá, Colombia
2018

Extended modules over skew PBW extensions

William Alfredo Fajardo Cardenas

Thesis Work to Obtain the degree of:
Doctor of Science in Mathematics

Advisor:
Ph.D., Oswaldo Lezama

Line of research:
Algebra
Research group:
SAC^2

Universidad Nacional de Colombia
Facultad de Ciencias, Departamento de Matemáticas
Bogotá, Colombia
2018

Dedicated to

My parents and sisters.

Acknowledgements

Thank very much to my tutor, Professor José Oswaldo Lezama Serrano. Thank to him for his patience, dedication, motivation, criterion and encourage for to continue. He is one who has made the difficult thing easy. It has been a privilege to be able to rely on his guide and help. I also thank to Sciences School of National University of Colombia for their support. Thanks to all the persons of the National University of Colombia for their attention and amiability in everything relating to my life like pupil of doctorate.

The received love, the dedication and the patience with which every day my parents were worrying for my advance and development of this thesis, it is simply unique and is reflected in the life of a son.

Thanks to my parents and sisters for being the principal promoters of my dreams, thanks to them for every day to count and to believe in me and in my expectative, thanks to my mother for accompanying in this process that I reach, thanks to my father for being forever to want and to long the best thing for my life, thanks for every advice and them words that they have guided during my life.

Abstract

In the book "Serre's problem on projective modules" [42], Tsit Yuen Lam defines the class $\mathcal{E}$ of extended rings; these rings satisfy the extended version of the Quillen-Suslin theorem. In this thesis we investigate extended modules and rings for skew PBW extensions from a matrix-constructive approach. We determine conditions on the parameters that define a skew extension $A = \sigma(R)\langle x_1, \ldots, x_n\rangle$ in order to A be projective-free ($\mathcal{PF}$), or more generally, extended ($\mathcal{E}$). Under such particular conditions we prove Vaserstein's, Quillen's patching, Horrocks' and Quillen-Suslin's theorems for this type of non-commutative rings of polynomial type. Complementary, but as a very important part of the thesis, a computational package has been developed not only for the computations involved in the matrix-constructive proofs related to the $\mathcal{PF}$ and $\mathcal{E}$ properties, but also for many homological applications of the Gröbner theory of skew PBW extensions developed recently in many papers.

Keywords: Extended modules, extended rings, skew PBW extensions, Bass-Quillen conjecture, Quillen-Suslin theorem, matrix-constructive and algorithmic proofs, Gröbner basis, computational package for skew PBW extensions.

Resumen

En el libro "Serre's problem on projective modules" [42], Tsit Yuen Lam definió las clases $\mathcal{E}$ de anillos extendidos; estas clases de anillos satisfacen la versión extendida del teorema de Quillen-Suslin. En esta tesis investigamos módulos y anillos extendidos para extensiones PBW torcidas desde una aproximación matricial. Determinamos condiciones sobre los parámetros que definen una extensión torcida $A = \sigma(R)\langle x_1, \ldots, x_n\rangle$ para que A sea proyectivo-libre ($\mathcal{PF}$), o más general, extendida ($\mathcal{E}$). Bajo tales condiciones particulares nosotros probamos los teoremas de Vaserstein, patching de Quillen, Horrocks y Quillen-Suslin para este tipo de anillos polinomiales no conmutativos. Como complemento, pero como una muy importante parte de la tesis, algunos paquete han sido desarrollados no solo para cálculos que envueltos en la prueba matricial constructiva relacionada a las propiedades $\mathcal{PF}$ y $\mathcal{E}$, sino también para algunas aplicaciones homológicas de la teoría de bases de Gröbner de extensiones PBW torcidas desarrolladas recientemente en muchos trabajos.

Palabras clave: Módulos extendidos, anillos extendidos, extensiones PBW torcidas, conjetura de Bass-Quillen, teorema de Quillen-Suslin, aproximación matricial-constructiva y pruebas algorítmicas, bases de Gröbner, paquetes computacionales para extensiones PBW torcidas.

Content

Index of symbols

$\sigma(R)\langle x_1, \dots, x_n\rangle = \sigma(R)\langle X\rangle$	Skew PBW extension over a ring R
R^*	Multiplicative group of invertible elements of R
id_X	Identity function over a set X
$Q(R)$	Total ring of fractions of a ring R
$S^{-1}R$	Left localization of R by a multiplicative system S
RS^{-1}	Right localization of R by a multiplicative system S

$\mathfrak{M}(R)$	Family of finitely generated left R-modules
$\mathfrak{P}(R)$	Family of finitely generated projective left R-modules
$\mathfrak{M}^L(T)$	Left T-modules in $\mathfrak{M}(T)$ extended from L
$\mathfrak{P}^L(T)$	Left T-modules in $\mathfrak{P}(T)$ extended from L.
$M[T]$	The $R[T]$-module $R[T] \otimes_R M$
$M\langle T\rangle$	The $R\langle T\rangle$-module $R\langle T\rangle \otimes_{R[T]} M$

$\mathcal{RC}$	Class of rings satisfying the property $\mathcal{RC}$
$\mathcal{IBN}$	Class of rings satisfying the invariant basis number property
$\mathcal{LGS}$	Class of left Gröbner soluble rings
$\mathcal{E}$	Class of skew PBW extensions $A = \sigma(R)\langle X\rangle$ extended from R
$\mathcal{PF}$	Class of rings R such that every $M \in \mathfrak{P}(R)$ is R-free
$\mathcal{PSF}$	Class of rings R such that every $M \in \mathfrak{P}(R)$ is stably free R-module
$\mathcal{H}$	Class of Hermite rings

$\mathcal{M}_{m\times n}(R)$	Set of matrices of size $m \times n$ over ring R
$\mathcal{M}_n(R)$	Ring of matrices of size $n \times n$ over ring R
$\mathrm{GL}_n(R)$	General linear group of dimension n over ring R
$\mathrm{SL}_n(R)$	Special linear group of dimension n over ring R
$A \sim B$	Matrix A is similar to matrix B

PID	Principal ideal domain

$Mon(A)$	Set of monomials of a skew PBW extension A
$exp(X)$	Exponent of a monomial X in $Mon(A)$
$lcm(X, Y)$	Least common multiple of monomials X, Y in $Mon(A)$
$lm(f)$	Leading monomial of a polynomial f in a skew PBW extension A
$lc(f)$	Leading coefficient of a polynomial f in a skew PBW extension A
$lt(f)$	Leading term of a polynomial f in a skew PBW extension A
$t(f)$	Finite set of terms that conform a polynomial f
$deg(X)$	$\|\alpha\| = \alpha_1 + \cdots + \alpha_n$, where $X := x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in Mon(A)$
$deg(f)$	$max(deg(X_i))_{i=1}^{t}$, where $f = c_1X_1 + \cdots + c_tX_t$, with $X_i \in Mon(A)$
$x^\alpha \| x^\beta$	x^α divide x^β, where $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $x^\beta = x_1^{\beta_1} \cdots x_n^{\beta_n} \in Mon(A)$

$Mon(A^m)$	Set of monomials of A^m, where A is a skew PBW extension
$\mathbf{e}_i$	i-th canonical vector of A^m
$\boldsymbol{X}$	Monomial $X\mathbf{e}_i$ in A^m, where X in $Mon(A)$
$exp(\boldsymbol{X})$	Exponent of a monomial $\boldsymbol{X}$ in $Mon(A^m)$
$lcm(\boldsymbol{X}, \boldsymbol{Y})$	Least common multiple of monomials $\boldsymbol{X}$, $\boldsymbol{Y}$ in $Mon(A^m)$
$lm(\boldsymbol{f})$	Leading monomial of a polynomial $\boldsymbol{f}$ in A^m
$lc(\boldsymbol{f})$	Leading coefficient of a polynomial $\boldsymbol{f}$ in A^m
$lt(\boldsymbol{f})$	Leading term of a polynomial $\boldsymbol{f}$ in A^m
$t(\boldsymbol{f})$	Finite set of terms that conform a polynomial $\boldsymbol{f}$
$deg(\boldsymbol{X})$	$\|\alpha\| = \alpha_1 + \cdots + \alpha_n$, where $\boldsymbol{X} := x_1^{\alpha_1} \cdots x_n^{\alpha_n}\boldsymbol{e}_i \in Mon(A^m)$
$deg(\boldsymbol{f})$	$max(deg(\mathbf{X}_i))_{i=1}^{t}$, where $\boldsymbol{f} = c_1\boldsymbol{X}_1 + \cdots + c_t\boldsymbol{X}_t$, with $\boldsymbol{X}_i \in Mon(A^m)$
$\boldsymbol{X} \| \boldsymbol{Y}$	$\boldsymbol{X}$ divide $\boldsymbol{Y}$, where $\boldsymbol{X}$, $\boldsymbol{Y} \in Mon(A^m)$

$\langle f_1, \ldots, f_s\}$	Left ideal generated by $\{f_1, \ldots, f_s\}$
$\langle \boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\rangle$	Submodule generated by $\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\}$
$Syz_R(f_1, \ldots, f_m)$	left R-module $\{(b_1, \ldots, b_m) \in R^m \| \, b_1f_1 + \cdots + b_mf_m = 0\}$
$Syz(f_1, \ldots, f_m)$	$Syz_A(f_1, \ldots, f_m)$, where A is a skew PBW extension
$Syz_R(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m)$	left R-module $\{(b_1, \ldots, b_m) \in R^m \| \, b_1\boldsymbol{f}_1 + \cdots + b_m\boldsymbol{f}_m = \boldsymbol{0}\}$
$Syz(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m)$	$Syz_A(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m)$, where A is a skew PBW extension

Introduction

The extended modules emerged as a result of Serre's classic problem that asks if R is a field and $A := R[x_1, \ldots, x_n]$ is the ring of polynomials in n indeterminate over R, then every finitely generated projective module over A is free? In 1976 Quillen and Suslin discovered independently positive proofs of this problem. Moreover, their methods showed that the conjecture is also valid if R is a principal ideal domain (DIP), and more strongly, when R is a Dedekind domain, then all finitely generated projective modules over A are extended from R ([42], [22]).
The main purpose of this thesis is to study the extended modules over some classes of skew PBW extensions; these type of noncommutative rings of polynomial type were defined in 2011 by Gallego and Lezama in [26] and have been enough studied since then (see [1], [2], [3], [7], [19], [26], [27], [28], [39], [45], [46], [47], [48], [49], [65], [66], [67], [73], [74], [76]). Given a skew PBW extension A of a R ring, a left A-modulo P is called *extended from* R if there is a left R-modulo P_0 such that $P \cong A \otimes_R P_0$.
Finitely generated projective modules have investigated for many authors for some particular classes of noncommutative algebras as Weyl algebras, enveloping algebras of Lie algebras, quantum polynomials, among many others (see [9], [10], [11], [12], [13], [18], [20], [34], [64], [71], [72]). However, the extended modules for noncommutative rings and algebras have not been enough studied.
The main results on the notion of extended modules are reduced to the commutative case. One of the first results for the case of R non-Noetherian was "hidden" in an investigation published in 1971. In a short summary in the AMS Notices, W. V. Vasconcelos and A. Simis established that if R is a valuation domain then every finitely generated projective module on $R[x]$ is free [75]. Nothing was said about the multivariate case, and the details of the univariate case proof were not published, for this fact it is said that the result was "hidden". After solving the Serre conjecture by Quillen and Suslin, the work was also initiated for the coefficient case in a non-Noetherian ring. Brewer and Costa showed in 1978 (see [16]), that if N is the nilradical of a commutative ring R and if each finitely generated projective module P over $R[x_1, \ldots, x_n]$ is extended from R, then P/NP is extended from R/N. Using this result, Brewer and Costa showed that if R is a Prüfer domain with Krull dimension ≤ 1, then each finitely generated projective module over the ring $R[x_1, \ldots, x_n]$ is extended from R. Using a modification of Quillen's induction theorem, in 1980 Lequain and Simis extended the Brewer and Costa result to any Prüfer domain ([43]). Several researchers have used in their works the Quillen's induction or the Lequain and Simis' induction in the investigation of extended modules and rings.
A branch of research around the generalization of the Quillen-Suslin theorem is aimed at presenting constructive methods; authors such as Henry Lombardi ([56], [57], [58], [59]) and Ihsen Yengui ([79], [80]) developed this methodology. These authors presented con-

structive approaches to the versions of the Quillen-Suslin theorem for extended modules on non-noetherian rings, for example, for coherent rings with dimension of Krull ≤ 1. They implemented arithmetic characterizations of these rings and use the local-global principles, defining constructively concepts or proofs such as the Krull dimension, the Quillen's patching, the Quillen's induction, among others.

Many questions arise when modules and rings are investigated. The proposal of this thesis is focused on the following aspects:

(a) Study from a matrix-constructive approach for special classes of skew PBW extensions some theorems that come from commutative homological algebra, theorems that play a fundamental role in the investigation of noncommutative version of the Quillen-Suslin theorem, the Bass-Quillen conjecture, and in general, in the investigation of extended modules and rings. Such theorems are Vaserstein's theorem, Quillen's patching and Horrocks' theorem. It is important to remark that in [12] Quillen's patching theorem and the Horrocks' theorem were studied for quantum polynomials, which also correspond to locations of appropriate skew PBW extensions (see [48], [50]). Paper [12] was the main motivation for the present research.

(b) In order to complement the matrix-constructive study of extended modules in (a), we have implemented in Maple the theory of Gröbner basis of skew PBW extensions, as well as, some of its applications in homological algebra. This is a very important part of the thesis since it is useful not only for investigating constructively homological properties of many algebras that can be described as skew PBW extensions, but also for many eventual applications of them (see for example Chapter 3).

The present monograph is organized in the following way: In the first chapter we present some preliminaries of homological algebra, in particular, we recall the definition of the following classes of rings related to rings $\mathcal{E}$ ([46]): $\mathcal{RC}$, $\mathcal{IBN}$, $\mathcal{PF}$, $\mathcal{PSF}$, $\mathcal{H}$. For the $\mathcal{PF}$ rings we recall its constructive matrix characterization (Theorem 1.1.3). We present also a matrix interpretation of isomorphic modules that will be used in the second chapter. In this first chapter we also recall the definition of the skew PBW extensions and we give some properties of them such as: The Hilbert basis theorem (Theorem 1.3.9), Serre's theorem (Theorem 1.3.10) and some important facts about locations. Within the preliminaries are also included well-known results about Gröbner bases for bijective skew PBW extensions, these results are fundamental in the implementation. Finally, the chapter concludes with some results about syzygy modules and free resolutions.

The contributions of the present investigation are concentrated in Chapters 2, 3 and 4. The second chapter is dedicated to investigate the extended modules and the key theorems related with them for a restricted class of skew PBW extension, namely, for Ore extensions of the form $R[x_1, \ldots, x_n; \sigma]$, where R is a commutative ring and σ an automorphism of R. The main results are: Theorem 2.2.3, Proposition 2.2.5, Proposition 2.2.7 and Corollary 2.2.8, which are generalizations of the classical commutative case; Theorem 2.2.3 is a matrix interpretation of the extended modules. In this chapter we also include the Vaserstein's theorem (Theorem 2.3.3), which is an adaptation of the commutative case ([41]); we also present a result that is of vital importance in the Quillen's induction, the Quillen's patching theorem (Theorem 2.4.1). Theorem 2.5.3 is a noncommutative version of Quillen-Suslin theorem for Ore extensions. Finally, the chapter concludes with a constructive proof of the

Quillen-Suslin theorem for the skew polynomial ring $K[x_1; \sigma, \delta]$, where K is a division ring, σ is automorphism on K and δ is a σ-derivation.
Chapter 3 contains an interesting application in multidimensional ideal code of the multivariable Ore extension $A[x_1, \ldots, x_n; \sigma]$, where A is a semisimple algebra and assuming some suitable conditions of separability. This application was obtained as an easy adaptation of works [31], [32] and [33], where the only one variable is studied.
In the fourth chapter we present the implementation developed in Maple, this implementation is based on a library specialized for working with skew PBW extensions. The library has utilities to calculate Gröbner bases over bijective kew PBW extensions, moreover, it includes some functions that calculate: The module of syzygies, free resolutions and left inverses of matrices, among others. In addition, we create another independent library that allows to execute the Quillen-Suslin theorem for $K[x; \sigma, \delta]$, with K a field, σ a K-automorphism and δ a σ-derivation.
In appendices A and B we present the documentation and content of the library SPBWE.lib developed in Maple, in Appendix A we present the packages: SPBWETools, RingTools and SPBWEGrobner, these contain utilities to define and perform calculations with PBW extensions, in Appendix B the package `SPBWERings` is presented, which contains a list of skew PBW extensions that are predefined in the library.
There are available many computational packages that make computations with noncommutative algebras of polynomial type, among them we can mention the following:

J. Apel and U. Klaus ([6], http://felix.hgb-leipzig.de)

MAS by H. Kredel and M. Pesch ([40], http://krum.rz.uni-mannheim.de/mas.html)

Singular:Plural by V. Levandovskyy et al. ([36], http://www.singular.uni-kl.de)

Macaulay2 by D. Grayson and M. Stillman (http://www.math.uiuc.edu/Macaulay2, ([35])

Kan/sm1 by N. Takayama et. al.

However none of the above systems make computations with skew PBW extensions, so the package developed represent a novelty.

1. Preliminaries

In this introductory chapter we present the basic algebraic tools that we will use in the thesis, in particular, we recall some well-known facts about the matrix interpretation of finitely generated projective modules over arbitrary noncommutative rings, as well as, some remarks about the matrix interpretation of isomorphic modules over arbitrary rings. A very important section about the skew PBW extensions and its Gröbner theory is included.

1.1. $\mathcal{PF}$, $\mathcal{PSF}$ and $\mathcal{H}$ rings

In this first section we recall some classes of rings closed related to the extended rings, which are the central topic of this monograph (see [46]).

Definition 1.1.1. *Let R be a ring.*

(i) R is an $\mathcal{RC}$ ring if for any integers $s, t \geq 1$, given an epimorphism $R^s \to R^t$, then $s \geq t$.

(ii) R is an $\mathcal{IBN}$ ring (Invariant Basis Number) if for any integers $s, t \geq 1$, $R^s \cong R^t$ if and only if $s = t$.

All rings considered in this monograph are $\mathcal{RC}$, and hence $\mathcal{IBN}$ ([46] Section 1, Proposition 3).

Definition 1.1.2.

(i) A ring R is a $\mathcal{PF}$ ring if every finitely generated projective R-module is free.

(ii) A ring R is a $\mathcal{PSF}$ ring if every finitely generated projective R-module is stably free, i.e., for every finitely generated projective R-module M there exist $n, m \in \mathbb{Z}^+ \cup \{0\}$ such that $R^n \oplus M \cong R^m$.

(iii) A ring is $\mathcal{H}$ (Hermite ring, see [42]) if every stably free R-module is free.

The following matrix characterization of $\mathcal{PF}$ rings will be very important in what follows.

Theorem 1.1.3. *Let R be a ring. R is $\mathcal{PF}$ if and only if for every $s \geq 1$, given an idempotent matrix $F \in M_s(R)$, there exists a matrix $U \in GL_s(R)$ such that*

$$UFU^{-1} = \begin{bmatrix} 0 & 0 \\ 0 & I_r \end{bmatrix}, \tag{1-1}$$

where $r = dim(\langle F \rangle)$, $0 \leq r \leq s$, and $\langle F \rangle$ represents the left R-module generated by the rows of F. Moreover, a basis of M is given by the last r rows of U.

Proof. (See [46], Section 4, Corollary 7). □

1.2. Matrix interpretation of isomorphic modules

In this section we present some remarks about matrix interpretation of isomorphic modules over arbitrary rings; in [41] these remarks were considered for commutative rings, however the adaptation to the noncommutative case is direct. Anyway, we include the proofs for completeness.
Every ring homomorphism $R \longrightarrow T$ induce natural homomorphisms

$$\mathcal{M}_{m\times n}(R) \longrightarrow \mathcal{M}_{m\times n}(T), \qquad \mathrm{GL}_m(R) \longrightarrow \mathrm{GL}_m(T).$$

Definition 1.2.1. *Two matrices $F, G \in \mathcal{M}_{m\times n}(R)$ are equivalent (denoted $F \sim G$) if there exist $P \in \mathrm{GL}_m(R)$ and $Q \in \mathrm{GL}_n(R)$ such that*

$$F = PGQ.$$

Consider two exact sequences of R-modules

$$0 \to K_1 \xrightarrow{\beta_1} F_1 \xrightarrow{\alpha_1} M_1 \to 0$$
$$0 \to K_2 \xrightarrow{\beta_2} F_2 \xrightarrow{\alpha_2} M_2 \to 0,$$

where F_1, F_2 are free.

Proposition 1.2.2. *If $i : M_1 \longrightarrow M_2$ is an isomorphism, then there exists $\alpha \in \mathrm{Aut}(F_1 \oplus F_2)$ such that following diagram*

$$\begin{array}{ccc} F_1 \oplus F_2 & \xrightarrow{(\alpha_1,0)} & M_1 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle i} \\ F_1 \oplus F_2 & \xrightarrow[(0,\alpha_2)]{} & M_2 \end{array} \tag{1-2}$$

is commutative. Identifying K_j with $\beta_j(K_j) \subseteq F_j$ $(j = 1, 2)$, $\alpha(K_1 \oplus F_2) = F_1 \oplus K_2$.

Proof. Since F_j $(j = 1, 2)$ is free, we can define homomorphisms $\gamma_1 : F_1 \longrightarrow F_2$ and $\gamma_2 : F_2 \longrightarrow F_1$ such that the following diagrams commute

$$\begin{array}{ccc} F_1 & \xrightarrow{\alpha_1} & M_1 \\ \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle i} \\ F_2 & \xrightarrow[\alpha_2]{} & M_2 \end{array}$$

$$\begin{array}{ccc} F_1 & \xrightarrow{\alpha_1} & M_1 \\ \uparrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle i} \\ F_2 & \xrightarrow[\alpha_2]{} & M_2, \end{array}$$

We define

$\alpha' : F_1 \oplus F_2 \longrightarrow F_1 \oplus F_2,$ maps to $(x, y) \mapsto (x, y - \gamma_1(x)),$

$\alpha'' : F_1 \oplus F_2 \longrightarrow F_1 \oplus F_2,$ maps to $(x, y) \mapsto (x - \gamma_2(y), y).$

Note that α', $\alpha'' \in \mathrm{Aut}(F_1 \oplus F_2)$. We want to show that $\alpha := \alpha'^{\,-1} \circ \alpha''$ is the claimed isomorphism. Since

$$(i\alpha_1, \alpha_2)(\alpha''(x, y)) = i\alpha_1(x) - i\alpha_1\gamma_2(y) + \alpha_2(y) = i\alpha_1(x) = i \circ (\alpha_1, 0)(x, y)$$

and

$$(i\alpha_1, \alpha_2)(\alpha'(x, y)) = i\alpha_1(x) + \alpha_2(y) - \alpha_2\gamma_1(x) = (0, \alpha_2)(x, y),$$

then $(0, \alpha_2) \circ \alpha = i \circ (\alpha_1, 0)$ since $\alpha'' = \alpha' \circ \alpha$.
For the second statement of (i), we have $K_1 \oplus F_2 = \ker(\alpha_1, 0)$ and $F_1 \oplus K_2 = \ker(0, \alpha_2)$, therefore $\alpha(K_1 \oplus F_2) = F_1 \oplus K_2$. Indeed, $(0, \alpha_2) \circ \alpha(K_1 \oplus F_2) = i \circ (\alpha_1, 0)(K_1 \oplus F_2) = 0$, so $\alpha(K_1 \oplus F_2) \subseteq \ker(0, \alpha_2) = F_1 \oplus K_2$; for the other inclusion we have $(\alpha_1, 0)\alpha^{-1}(F_1 \oplus K_2) = i^{-1}(0, \alpha_2)(F_1 \oplus K_2) = 0$, whence $\alpha^{-1}(F_1 \oplus K_2) \subseteq \ker(\alpha_1, 0) = K_1 \oplus F_2$, i.e., $F_1 \oplus K_2 \subseteq \alpha(K_1 \oplus F_2)$. □

From the previous proposition we get the following interesting result.

Corollary 1.2.3. *Let R be a ring and consider two exact sequences of R-modules*

$$F_j' \xrightarrow{\beta_j} F_j \xrightarrow{\alpha_j} M_j \longrightarrow 0 \qquad (j = 1, 2), \tag{1-3}$$

where F_j, F_j' are free $R-$modules. Then, $M_1 \cong M_2$ if and only if there exist $\alpha \in \mathrm{Aut}(F_1 \oplus F_2)$ and $\beta \in \mathrm{Aut}(F_1' \oplus F_2 \oplus F_1 \oplus F_2')$ such that the following diagram

$$\begin{array}{ccc} F_1' \oplus F_2 \oplus F_1 \oplus F_2' & \xrightarrow{(\beta_1 \oplus i_{F_2}, 0)} & F_1 \oplus F_2 \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} \\ F_1' \oplus F_2 \oplus F_1 \oplus F_2' & \xrightarrow[(0, i_{F_1} \oplus \beta_2)]{} & F_1 \oplus F_2 \end{array} \tag{1-4}$$

commutes.

Proof. $\Rightarrow$): Assume that $M_1 \cong M_2$ and let $K_j := \ker(\alpha_j) = Im(\beta_j)$ $(j = 1, 2)$. By Proposition 1.2.2, there exists $\alpha \in \mathrm{Aut}(F_1 \oplus F_2)$ and an isomorphism α' such that the diagram

$$\begin{array}{ccccc} F_1' \oplus F_2 & \xrightarrow{\beta_1 \oplus i_{F_2}} & K_1 \oplus F_2 & \xrightarrow{\iota_1} & F_1 \oplus F_2 \\ & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} \\ F_1 \oplus F_2' & \xrightarrow{i_{F_1} \oplus \beta_2} & F_1 \oplus K_2 & \xrightarrow{\iota_2} & F_1 \oplus F_2 \end{array}$$

commutes, where ι_1, ι_2 are the inclusions. Applying again Proposition 1.2.2 to isomorphism α', we obtain the isomorphism β making diagram (1-4) commutative.
$\Leftarrow$): In the diagram (1-4), $(\beta_1 \oplus i_{F_2}, 0)$ coincides with β_1 on F_1', with i_{F_2} on F_2 and with 0 on F_1 and F_2'. In a similar way is defined $(0, \mathrm{id}_{F_1} \oplus \beta_2)$. From (1-4) we obtain that $M_1 \cong M_2$. This is because $M_1 \cong coker(\beta_1 \oplus i_{F_2}, 0)$ and $M_2 \cong coker(i_{F_1} \oplus \beta_2)$. In fact, for example, $F_1 \oplus F_2/Im(\beta_1 \oplus i_{F_2}, 0) = F_1 \oplus F_2/K_1 \oplus F_2 \cong F_1/K_1 \cong F_1/\ker(\alpha_1) \cong M_1$. □

Now we can consider that M_1 and M_2 are finitely presented R-modules,

$$F_1' \xrightarrow{\beta_1} F_1 \xrightarrow{\alpha_1} M_1 \to 0$$
$$F_2' \xrightarrow{\beta_2} F_2 \xrightarrow{\alpha_2} M_2 \to 0.$$

With respect to the canonical basis, β_1 is given by a matrix $B_1 \in M_{m'\times m}(R)$ and β_2 by $B_2 \in M_{n'\times n}(R)$. The matrices that represent the homomorphisms in the rows of (1-4) are given by

$$\left[\begin{array}{c|c} B_1 & 0 \\ \hline 0 & I_n \\ \hline \multicolumn{2}{c}{0} \end{array}\right] \quad \text{and} \quad \left[\begin{array}{c|c} \multicolumn{2}{c}{0} \\ \hline I_m & 0 \\ \hline 0 & B_2 \end{array}\right], \tag{1-5}$$

which are in $M_{r\times s}(R)$, where $r := m + n + m' + n'$ and $s := m + n$. Therefore, Corollary 1.2.3 says that the modules M_1 and M_2 are isomorphic if and only if the matrices in (1-5) are equivalent.

1.3. Skew PBW extensions

The modules studied in this thesis are over skew PBW extensions; this class of noncommutative rings of polynomial type were introduced in [26]. We will recall its definition and some key properties.

Definition 1.3.1. *Let R and A be rings, we say that A is a skew PBW extension of R also called σ-PBW extension, if the following conditions hold:*

(i) $R \subseteq A$.

(ii) There exist finitely many elements $x_1, \dots, x_n \in A$ such that A is a left R-free module with basis

$$Mon(A) := Mon\{x_1, \dots, x_n\} = \{x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n} | \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n\}.$$

(iii) For every $1 \le i \le n$ and $r \in R - \{0\}$ there exists $c_{i,r} \in R - \{0\}$ such that

$$x_i r - c_{i,r} x_i \in R. \tag{1-6}$$

(iv) *For every $1 \leq i < j \leq n$ there exists $c_{i,j} \in R$ left invetible such that*

$$x_j x_i - c_{i,j} x_i x_j \in R + Rx_1 + \cdots + Rx_n. \tag{1-7}$$

Under these conditions we will write $A = \sigma(R)\langle x_1, \ldots, x_n \rangle$, and R will be called the ring of coefficients of the extension.

Remark 1.3.2. (i) In general, for $i \neq j$ the elements x_i and x_j do not commute. Since that $Mon(A)$ is a R-basis for A, in the above definition the elements $c_{i,r}$ and $c_{i,j}$ are unique.
(ii) If $r = 0$, then we define $c_{i,0} = 0$: In fact, $0 = x_i 0 = c_{i,0} x_i + s_i$, with $s_i \in R$, but since $Mon(A)$ is a R-basis, then $c_{i,0} = 0 = s_i$.
(iii) Comparing with [26], i.e., assuming in (iv) of the previous definition only that $c_{ij} \neq 0$ for all $1 \leq i, j \leq n$, then there exist $c_{j,i}, c_{i,j} \in R$ such that $x_i x_j - c_{j,i} x_j x_i \in R + Rx_1 + \cdots + Rx_n$ and $x_j x_i - c_{i,j} x_i x_j \in R + Rx_1 + \cdots + Rx_n$, but since $Mon(A)$ is a R-basis then $1 = c_{j,i} c_{i,j}$, whence, for every $1 \leq i < j \leq n$, $c_{i,j}$ is left invertible; moreover, $c_{i,i} = 1$: In fact, $x_i^2 - c_{i,i} x_i^2 = s_0 + s_1 x_1 + \cdots + s_n x_n$, with $s_i \in R$, hence $1 - c_{i,i} = 0 = s_i$.
(iv) The elements of $Mon(A)$ will be denoted also in capital letters, thus, $x^\alpha \in Mon(A)$ will be represented also as X if it is not important to highlight the exponents $\alpha_1, \ldots, \alpha_n$ in x^α.
(v) Each element $f \in A - \{0\}$ has a unique representation in the form $f = c_1 X_1 + \cdots + c_t X_t$, with $c_i \in R - \{0\}$ and $X_i \in Mon(A)$, $1 \leq i \leq t$.

Example 1.3.3. Many rings and algebras coming from mathematical physics can be described as skew PBW extensions, among of the most remarkable examples are: The usual polynomial ring, the enveloping algebra of a finite dimensional Lie algebra, the Weyl algebra, the additive analogue of the Weyl algebra, the algebra of q-differential operators, the algebra of shift operators, the algebra of linear partial shift operators, the algebra of linear partial difference operators, the algebra of linear partial q-differential operators, the algebra of linear partial q-dilation operators, the quantum polynomials, Ore algebras of bijective type, some diffusion algebras, the Woronowicz algebra, the dispin algebra, the coordinate algebra of the quantum matrix space, the q-Heisenberg algebra, the quantum enveloping algebra of $\mathfrak{sl}(2, K)$, the Hayashi algebra, the quantum Weyl algebra of Maltsiniotis, the Witten's deformation of $\mathcal{U}(\mathfrak{sl}(2, K)$, the quantum Weyl algebra $A_n(q, p_{i,j})$, the multiparameter quantized Weyl algebra $A_n^{Q,\Gamma}(K)$, the quantum symplectic space $\mathcal{O}_q(\mathfrak{sp}(K^{2n}))$, some quadratic algebras in three variables. For a precise definition of these algebras see [48].

The following proposition is fundamental.

Proposition 1.3.4. *Let A be a skew PBW extension of R. Then, for every $1 \leq i \leq n$, there exist an injective ring endomorphism $\sigma_i : R \to R$ and a σ_i-derivation $\delta_i : R \to R$ such that*

$$x_i r = \sigma_i(r) x_i + \delta_i(r),$$

for each $r \in R$.

Proof. (See [26] Proposition 13). □

A particular class of skew PBW extension is when all derivations δ_i are zero. Another interesting case is when all σ_i are bijective and the constants c_{ij} are invertible. We have the following definition.

Definition 1.3.5. *Let A be a skew PBW extension.*

(a) A is quasi-commutative if the conditions ((iii)) and (iv) in Definition 1.3.1 are replaced by

(iii′) For every $1 \leq i \leq n$ and $r \in R - \{0\}$ there exists $c_{i,r} \in R - \{0\}$ such that

$$x_i r = c_{i,r} x_i. \tag{1-8}$$

(iv′) For every $1 \leq i, j \leq n$ there exists $c_{i,j} \in R - \{0\}$ such that

$$x_j x_i = c_{i,j} x_i x_j. \tag{1-9}$$

(b) A is bijective if σ_i is bijective for every $1 \leq i \leq n$ and $c_{i,j}$ is invertible for any $1 \leq i < j \leq n$.

Remark 1.3.6. We observe if A is quasi-commutative, then the evaluation function at 0, i.e., $A \to R$, $f \in A \mapsto f(0) \in R$, is a surjective ring homomorphism with kernel $\langle x_1, \ldots, x_n \rangle$, the two-sided ideal generated by $x_1, \ldots, x_n$. Thus, $A/\langle x_1, \ldots, x_n \rangle \cong R$ as rings.

Definition 1.3.7. *Let A be a skew PBW extension of R with endomorphisms σ_i, $1 \leq i \leq n$, as in Proposition 1.3.4.*

(i) For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $\sigma^\alpha := \sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n}$, $|\alpha| := \alpha_1 + \cdots + \alpha_n$. If $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$, then $\alpha + \beta := (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$.

(ii) For $X = x^\alpha \in Mon(A)$, $\exp(X) := \alpha$ and $\deg(X) := |\alpha|$.

(iii) Let $0 \neq f \in A$, $t(f)$ is the finite set of terms that conform f, i.e., if $f = c_1 X_1 + \cdots + c_t X_t$, with $X_i \in Mon(A)$ and $c_i \in R - \{0\}$, then $t(f) := \{c_1 X_1, \ldots, c_t X_t\}$.

(iv) Let f be as in (iii), then $\deg(f) := \max\{\deg(X_i)\}_{i=1}^{t}$.

The skew PBW extensions can be characterized in a similar way as was done in [17] for PBW rings.

Theorem 1.3.8. *Let A and R be rings satisfying the condition (i)-(ii) of Definition 1.3.1. A is a skew PBW extension of R if and only if the following conditions hold:*

(a) For every $x^\alpha \in Mon(A)$ and every $0 \neq r \in R$ there exist unique elements $r_\alpha = \sigma^\alpha(r) \in R - \{0\}$ and $p_{\alpha,r} \in A$ such that

$$x^\alpha r = r_\alpha x^\alpha + p_{\alpha,r}, \tag{1-10}$$

where $p_{\alpha,r} = 0$ or $\deg(p_{\alpha,r}) < |\alpha|$ if $p_{\alpha,r} \neq 0$. Moreover, if r is left invertible, then r_α is left invertible.

(b) For every $x^{\alpha}, x^{\beta} \in Mon(A)$ there exist unique elements $c_{\alpha,\beta} \in R$ and $p_{\alpha,\beta} \in A$ such that

$$x^{\alpha}x^{\beta} = c_{\alpha,\beta}x^{\alpha+\beta} + p_{\alpha,\beta}, \tag{1-11}$$

where $c_{\alpha,\beta}$ is left invertible, $p_{\alpha,\beta} = 0$ or $\deg(p_{\alpha,\beta}) < |\alpha+\beta|$ if $p_{\alpha,\beta} \neq 0$.

Skew PBW extensions have been intensively investigated in recent papers (see [1], [2], [3], [19], [26], [27], [28], [39], [45], [46], [47], [48], [49], [65], [66], [73], [74], [76], among many others). Next we present some of the most important important ring theoretic and homological properties of these noncommutative rings of polynomial type that we will use in this monograph.

Theorem 1.3.9 (Hilbert Basis Theorem, [48])**.** *Let A be a bijective skew PBW extension of R. If R is a left (right) Noetherian ring then A is also a left (right) Noetherian ring.*

Recall that a ring R is left (right) regular if every finitely generated left (right) R-module has finite projective dimension (see [64]).

Theorem 1.3.10 (Serre's theorem, [48])**.** *Let A be a bijective skew PBW extension of a ring R such that R is left (right) Noetherian, left (right) regular and $\mathcal{PSF}$. Then A is $\mathcal{PSF}$.*

Lemma 1.3.11 ([2])**.** *Let $A := R[z_1; \sigma_1] \cdots [z_n; \sigma_n]$ be a quasi-commutative skew PBW extension of a ring R and let S be a multiplicative system of R.*

(a) If $S^{-1}R$ exists and $\sigma_i(S) \subseteq S$ for every $1 \leq i \leq n$, then $S^{-1}A$ is a quasi-commutative skew PBW extension of RS^{-1} and

$$S^{-1}A \cong (S^{-1}R)[z_1; \overline{\sigma_1}] \cdots [z_n; \overline{\sigma_n}].$$

In addition, if A is bijective with $\sigma_i(S) = S$ for every i, then $S^{-1}A$ is a quasi-commutative bijective skew PBW extension of $S^{-1}R$.

(b) If RS^{-1} exists and A is bijective with $\sigma_i(S) = S$ for every $1 \leq i \leq n$, then AS^{-1} is a quasi-commutative bijective skew PBW extension of RS^{-1} and

$$AS^{-1} \cong (RS^{-1})[x_1; \widetilde{\sigma_1}] \cdots [x_n; \widetilde{\sigma_n}].$$

(c) If $S^{-1}R$ and RS^{-1} exist and A is bijective with $\sigma_i(S) = S$ for every $1 \leq i \leq n$, then $S^{-1}A \cong AS^{-1}$ is a quasi-commutative bijective skew PBW extension of $S^{-1}R \cong RS^{-1}$.

For the bijective case we have the next result, where $S_0(R)$ is the set of regular elements of R.

Theorem 1.3.12 ([2])**.** *Let R be a ring and $A := \sigma(R)\langle x_1, \ldots, x_n\rangle$ be a bijective skew PBW extension of R. Let $S \subseteq S_0(R)$ be a multiplicative subset of R such that $\sigma_i(S) = S$, for every $1 \leq i \leq n$, where σ_i is defined by Proposition 1.3.4.*

(i) *If $S^{-1}R$ exists, then $S^{-1}A$ exists and it is a bijective skew PBW extension of $S^{-1}R$ with*

$$S^{-1}A = \sigma(S^{-1}R)\langle x'_1, \ldots, x'_n\rangle,$$

where $x'_i := \frac{x_1}{1}$ and the system of constants of $S^{-1}R$ is given by $c'_{i,j} := \frac{c_{i,j}}{1}$, $c'_{i,\frac{r}{s}} := \frac{\sigma_i(r)}{\sigma_i(s)}$, $1 \leq 1, j \leq n$.

(ii) *If RS^{-1} exists, then AS^{-1} exists and it is a bijective skew PBW extension of RS^{-1} with*

$$AS^{-1} = \sigma(RS^{-1})\langle x''_1, \ldots, x''_n\rangle,$$

where $x''_i := \frac{x_i}{1}$ and the system of constants of RS^{-1} is given by $c''_{i,j} := \frac{c_{i,j}}{1}$, $c''_{i,\frac{r}{s}} := \frac{\sigma_i(r)}{\sigma_i(s)}$, $1 \leq 1, j \leq n$.

(iii) *If $S^{-1}R$ and RS^{-1} exist, then $S^{-1}A \cong AS^{-1}$ is a bijective skew PBW extension of $S^{-1}R \cong RS^{-1}$.*

Theorem 1.3.13 (Ore's theorem, [2])**.** *Let $A = \sigma(R)\langle x_1, \ldots, x_n\rangle$ be a bijective skew PBW extension of a left Ore domain R. Then A is also a left Ore domain, and hence, A has left total division ring of fractions such that*

$$Q_l(A) \cong Q_l(\sigma(Q_l(R))\langle x'_1, \ldots, x'_n\rangle).$$

If R is a right Ore domain, then A is also a right Ore domain, and hence, A has right total division ring of fractions such that

$$Q_r(A) \cong Q_r(\sigma(Q_r(R))\langle x''_1, \ldots, x''_n\rangle).$$

If R is an Ore domain (left and right), then A is an Ore domain and

$$Q(A) \cong Q(\sigma(Q(R))\langle x'_1, \ldots, x'_n\rangle) \cong Q(\sigma(Q(R))\langle x''_1, \ldots, x''_n\rangle).$$

1.4. Gröbner basis over skew PBW extensions

One of the main contributions of the present thesis is to implement in Maple the theory of Gröbner basis for modules over skew PB extensions. This implementation will be done in the last chapter. The theory was studied by Lezama-Gallego-Jiménez in some papers (see [25], [24], [26], [27], [39], [51]). We will review from [24], [27] and [45] the most basic definitions and facts of the Gröbner theory in order to understand better in the last chapter the implementation of the main algorithms involved in the theory, in particular, the Division Algorithm and the Buchberger Algorithm. The proofs omitted here can be found in the references cited above.

1.4.1. Monomial orders in skew PBW extensions

Let $A = \sigma(R)\langle x_1, \dots, x_n\rangle$ be a skew PBW extension of R and let $\succeq$ be a total order defined on $Mon(A)$. If $x^\alpha \succeq x^\beta$ but $x^\alpha \neq x^\beta$ we will write $x^\alpha \succ x^\beta$. $x^\beta \preceq x^\alpha$ means that $x^\alpha \succeq x^\beta$. Let $f \neq 0$ be a polynomial of A, if

$$f = c_1X_1 + \cdots + c_tX_t,$$

with $c_i \in R - \{0\}$ and $X_1 \succ \cdots \succ X_t$ are the monomials of f, then $lm(f) := X_1$ is the *leading monomial* of f, $lc(f) := c_1$ is the *leading coefficient* of f and $lt(f) := c_1X_1$ is the *leading term* of f. If $f = 0$, we define $lm(0) := 0, lc(0) := 0, lt(0) := 0$, and we set $X \succ 0$ for any $X \in Mon(A)$. Thus, we extend $\succeq$ to $Mon(A) \cup \{0\}$.

Definition 1.4.1. *Let $\succeq$ be a total order on $Mon(A)$, it is said that $\succeq$ is a monomial order on $Mon(A)$ if the following conditions hold:*

(i) For every $x^\beta, x^\alpha, x^\gamma, x^\lambda \in Mon(A)$

$$x^\beta \succeq x^\alpha \Rightarrow lm(x^\gamma x^\beta x^\lambda) \succeq lm(x^\gamma x^\alpha x^\lambda).$$

(ii) $x^\alpha \succeq 1$, for every $x^\alpha \in Mon(A)$.

(iii) $\succeq$ is degree compatible, i.e., $|\beta| \geq |\alpha| \Rightarrow x^\beta \succeq x^\alpha$.

The deglex order in $Mon(A)$ is defined by

$$x^\alpha \succeq x^\beta \iff \begin{cases} x^\alpha = x^\beta \\ or \\ x^\alpha \neq x^\beta \; but \, |\alpha| > |\beta| \\ or \\ x^\alpha \neq x^\beta, |\alpha| = |\beta| \; but \; \exists \; i \; with \quad \alpha_1 = \beta_1, \dots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i. \end{cases}$$

From now on we will assume that $Mon(A)$ is endowed with some monomial order.

Definition 1.4.2. *Let $x^\alpha, x^\beta \in Mon(A)$, we say that x^α divides x^β, denoted by $x^\alpha | x^\beta$, if there exists $x^\gamma, x^\lambda \in Mon(A)$ such that $x^\beta = lm(x^\gamma x^\alpha x^\lambda)$. We will say also that any monomial $x^\alpha \in Mon(A)$ divides the polynomial zero.*

Proposition 1.4.3. *Let $x^\alpha, x^\beta \in Mon(A)$ and $f, g \in A - \{0\}$. Then,*

(a) $lm(x^\alpha g) = lm(x^\alpha lm(g)) = x^{\alpha+\exp(lm(g))}$, i.e., $\exp(lm(x^\alpha g)) = \alpha + \exp(lm(g))$. In particular,

$$lm(lm(f)lm(g)) = x^{\exp(lm(f))+\exp(lm(g))}, \; i.e.,$$
$$\exp(lm(lm(f)lm(g))) = \exp(lm(f)) + \exp(lm(g))$$

and

$$lm(x^\alpha x^\beta) = x^{\alpha+\beta}, \; i.e., \; \exp(lm(x^\alpha x^\beta)) = \alpha + \beta. \tag{1-12}$$

(b) The following conditions are equivalent:

(i) $x^\alpha | x^\beta$.

(ii) There exists a unique $x^\theta \in Mon(A)$ *such that* $x^\beta = lm(x^\theta x^\alpha) = x^{\theta+\alpha}$ *and hence* $\beta = \theta + \alpha$.

(iii) There exists a unique $x^\theta \in Mon(A)$ *such that* $x^\beta = lm(x^\alpha x^\theta) = x^{\alpha+\theta}$ *and hence* $\beta = \alpha + \theta$.

(iv) $\beta_i \geq \alpha_i$ *for* $1 \leq i \leq n$, *with* $\beta := (\beta_1, \dots, \beta_n)$ *and* $\alpha := (\alpha_1, \dots, \alpha_n)$.

Some natural computational conditions on R will be assumed in this chapter (see [50]).

Definition 1.4.4. *A ring* R *is left Gröbner soluble (*$\mathcal{LGS}$*) if the following conditions hold:*

(i) R *is left Noetherian.*

(ii) Given $a, r_1, \dots, r_m \in R$ *there exists an algorithm which decides whether* a *is in the left ideal* $Rr_1 + \cdots + Rr_m$, *and if so, find* $b_1, \dots, b_m \in R$ *such that* $a = b_1r_1 + \cdots + b_mr_m$.

(iii) Given $r_1, \dots, r_m \in R$ *there exists an algorithm which finds a finite set of generators of the left* R*-module*

$$Syz_R[r_1 \ \cdots \ r_m] := \{(b_1, \dots, b_m) \in R^m | b_1r_1 + \cdots + b_mr_m = 0\}.$$

Remark 1.4.5. The three above conditions imposed to R are needed in order to guarantee a Gröbner theory in the rings of coefficients, in particular, to have an effective solution of the membership problem in R. **From now in this chapter on we will assume that** $A = \sigma(R)\langle x_1, \dots, x_n\rangle$ **is a bijective skew** PBW **extension of a** $\mathcal{LGS}$ **ring** R **and** $Mon(A)$ **is endowed with some monomial order**.

The Gröbner theory we are reviewing for modules, of course, includes the particular case of left ideals, however it is important to recall a couple of things of this particular situation.

Definition 1.4.6. *Let* $F := \{g_1, \dots, g_s\} \subseteq A$, X_F *the least common multiple of* $\{lm(g_1), \dots, lm(g_s)\}$, $\theta \in \mathbb{N}^n$, $\beta_i := \exp(lm(g_i))$ *and* $\gamma_i \in \mathbb{N}^n$ *such that* $\gamma_i + \beta_i = \exp(X_F)$, $1 \leq i \leq s$. $B_{F,\theta}$ *will denote a finite set of generators in* R^s *of*

$$S_{F,\theta} := Syz_R[\sigma^{\gamma_1+\theta}(lc(g_1))c_{\gamma_1+\theta,\beta_1} \ \cdots \ \sigma^{\gamma_s+\theta}(lc(g_s))c_{\gamma_s+\theta,\beta_s})].$$

For $\theta = \mathbf{0} := (0, \dots, 0)$, $S_{F,\theta}$ *will be denoted by* S_F *and* $B_{F,\theta}$ *by* B_F.

Remark 1.4.7. Let $(b_1, \dots, b_s) \in S_{F,\theta}$. Since A is bijective, then there exists an unique $(b'_1, \dots, b'_s) \in S_F$ such that $b_i = \sigma^\theta(b'_i)c_{\theta,\gamma_i}$ for $1 \leq i \leq s$: In fact, the existence and uniqueness of $(b'_1, \dots, b'_s)$ it follows from the bijectivity of A. Now, since $(b_1, \dots, b_s) \in S_{F,\theta}$, then $\sum_{i=1}^s b_i\sigma^{\theta+\gamma_i}(lc(g_i))c_{\theta+\gamma_i,\beta_i} = 0$. Replacing b_i by $\sigma^\theta(b'_i)c_{\theta,\gamma_i}$ in the last equation, we obtain $\sum_{i=1}^s \sigma^\theta(b'_i)c_{\theta,\gamma_i}\sigma^{\theta+\gamma_i}(lc(g_i)) \ c^{-1}_{\theta,\gamma_i}c_{\theta,\gamma_i}c_{\theta+\gamma_i,\beta_i} = 0$; multiplying by $c^{-1}_{\theta,\gamma_i+\beta_i}$ we get

$\sum_{i=1}^{s}\sigma^{\theta}(b'_i)c_{\theta,\gamma_i}\sigma^{\theta+\gamma_i}(lc(g_i))c^{-1}_{\theta,\gamma_i}c_{\theta,\gamma_i}c_{\theta+\gamma_i,\beta_i}\ c^{-1}_{\theta,\gamma_i+\beta_i}=0$; now we can use the identities of Remark 1.3.6, so

$$\sum_{i=1}^{s}\sigma^{\theta}(b'_i)\sigma^{\theta}(\sigma^{\gamma_i}(lc(g_i)))\sigma^{\theta}(c_{\gamma_i,\beta_i})=0,$$

and since σ^{θ} is injective then $\sum_{i=1}^{s}b'_i\sigma^{\gamma_i}(lc(g_i))c_{\gamma_i,\beta_i}=0$, i.e., $(b'_1,\dots,b'_s)\in S_F$.

The next theorem gives a matrix interpretation of the relation between the generators of a given left ideal I of A and its Gröbner basis.

Theorem 1.4.8 ([45])**.** *Let $F=\{f_1,\dots,f_s\}$ be a subset of A and $G=\{g_1,\dots,g_t\}$ be a Gröbner basis of $I:=\langle F\}$. Then, there exist matrices $H=[h_{ij}]\in M_{s\times t}(A)$ and $Q=[q_{ij}]\in M_{t\times s}(A)$ such that*

$$G^T=H^TF^T \text{ and } F^T=Q^TG^T,$$

where $G:=\begin{bmatrix}g_1 & \cdots & g_t\end{bmatrix}, F:=\begin{bmatrix}f_1 & \cdots & f_s\end{bmatrix}$ *and*

$$H:=\begin{bmatrix}h_{11} & \cdots & h_{1t}\\ \vdots & \ddots & \vdots\\ h_{s1} & \cdots & h_{st}\end{bmatrix} \text{ and } Q:=\begin{bmatrix}q_{11} & \cdots & q_{1s}\\ \vdots & \ddots & \vdots\\ q_{t1} & \cdots & q_{ts}\end{bmatrix}.$$

1.4.2. Gröbner basis of modules

Now we will review from ([27]) some basic definitions and facts of theory of Gröbner basis for submodules of A^m, $m\geq 1$, where $A=\sigma(R)\langle x_1,\dots,x_n\rangle$ is a bijective skew PBW extension of R, with R a $\mathcal{LGS}$ ring (see Definition 1.4.4) and $Mon(A)$ endowed with some monomial order (see Definition 1.4.1). A^m is the left free A-module of column vectors of length $m\geq 1$; since A is a left Noetherian ring (Theorem 1.3.9), then A is an IBN ring (Invariant Basis Number, see [53]), and hence, all basis of the free module A^m have m elements. The idea is recall the main notions of the Gröbner basis for submodules of A^m in order to understand better the implementaion in the last chapter of the Division Algorithm and the algorithm that computes the Gröbner basis using Maple.

Monomial orders on $Mon(A^m)$

We will often represent the elements of A^m also as row vectors, if this does not cause confusion. We recall that the canonical basis of A^m is

$$\boldsymbol{e}_1=(1,0,\dots,0),\boldsymbol{e}_2=(0,1,0,\dots,0),\dots,\boldsymbol{e}_m=(0,0,\dots,1).$$

Definition 1.4.9. *A monomial in A^m is a vector $\boldsymbol{X}=X\boldsymbol{e}_i$, where $X=x^{\alpha}\in Mon(A)$ and $1\leq i\leq m$, i.e.,*

$$\boldsymbol{X}=X\boldsymbol{e}_i=(0,\dots,X,\dots,0),$$

where X is in the i-th position, named the index of $\boldsymbol{X}$, $ind(\boldsymbol{X}) := i$. A term is a vector $c\boldsymbol{X}$, where $c \in R$. The set of monomials of A^m will be denoted by $Mon(A^m)$. Let $\boldsymbol{Y} = Y\boldsymbol{e}_j \in Mon(A^m)$, we say that $\boldsymbol{X}$ divides $\boldsymbol{Y}$ if $i = j$ and X divides Y. We will say that any monomial $\boldsymbol{X} \in Mon(A^m)$ divides the null vector $\mathbf{0}$. The least common multiple of $\boldsymbol{X}$ and $\boldsymbol{Y}$, denoted by $lcm(\boldsymbol{X}, \boldsymbol{Y})$, is $\mathbf{0}$ if $i \neq j$, and $U\boldsymbol{e}_i$, where $U = lcm(X, Y)$, if $i = j$. Finally, we define $\exp(\boldsymbol{X}) := \exp(X) = \alpha$ and $\deg(\boldsymbol{X}) := \deg(X) = |\alpha|$.

We now define monomial orders on $Mon(A^m)$.

Definition 1.4.10. *A monomial order on $Mon(A^m)$ is a total order $\succeq$ satisfying the following three conditions:*

(i) $lm(x^\beta x^\alpha)\boldsymbol{e}_i \succeq x^\alpha \boldsymbol{e}_i$, for every monomial $\boldsymbol{X} = x^\alpha \boldsymbol{e}_i \in Mon(A^m)$ and any monomial x^β in $Mon(A)$.

(ii) If $\boldsymbol{Y} = x^\beta \boldsymbol{e}_j \succeq \boldsymbol{X} = x^\alpha \boldsymbol{e}_i$, then $lm(x^\gamma x^\beta)\boldsymbol{e}_j \succeq lm(x^\gamma x^\alpha)\boldsymbol{e}_i$ for every monomial $x^\gamma \in Mon(A)$.

(iii) $\succeq$ is degree compatible, i.e., $\deg(\boldsymbol{X}) \geq \deg(\boldsymbol{Y}) \Rightarrow \boldsymbol{X} \succeq \boldsymbol{Y}$.

If $\boldsymbol{X} \succeq \boldsymbol{Y}$ but $\boldsymbol{X} \neq \boldsymbol{Y}$ we will write $\boldsymbol{X} \succ \boldsymbol{Y}$. $\boldsymbol{Y} \preceq \boldsymbol{X}$ means that $\boldsymbol{X} \succeq \boldsymbol{Y}$.

Proposition 1.4.11. *Every monomial order on $Mon(A^m)$ is a well order.*

Given a monomial order $\succeq$ on $Mon(A)$, we can define two natural orders on $Mon(A^m)$.

Definition 1.4.12. *Let $\boldsymbol{X} = X\boldsymbol{e}_i$ and $\boldsymbol{Y} = Y\boldsymbol{e}_j \in Mon(A^m)$.*

(i) The TOP (term over position) order is defined by

$$\boldsymbol{X} \succeq \boldsymbol{Y} \Longleftrightarrow \begin{cases} X \succeq Y \\ or \\ X = Y \, and \quad i > j. \end{cases}$$

(ii) The TOPREV order is defined by

$$\boldsymbol{X} \succeq \boldsymbol{Y} \Longleftrightarrow \begin{cases} X \succeq Y \\ or \\ X = Y \, and \quad i < j. \end{cases}$$

Remark 1.4.13. (i) Note that with TOP we have

$$\boldsymbol{e}_m \succ \boldsymbol{e}_{m-1} \succ \cdots \succ \boldsymbol{e}_1$$

and

$$\boldsymbol{e}_1 \succ \boldsymbol{e}_2 \succ \cdots \succ \boldsymbol{e}_m$$

for TOPREV.
(ii) The POT (position over term) and POTREV orders defined in [4] and [50] for modules over classical polynomial commutative rings are not degree compatible.
(iii) Other examples of monomial orders in $Mon(A^m)$ are considered in [18], e.g., orders with weights.

We fix a monomial order on $Mon(A)$, let $\boldsymbol{f} \neq \boldsymbol{0}$ be a vector of A^m, then we may write $\boldsymbol{f}$ as a sum of terms in the following way

$$\boldsymbol{f} = c_1\boldsymbol{X}_1 + \cdots + c_t\boldsymbol{X}_t,$$

where $c_1, \ldots, c_t \in R - 0$ and $\boldsymbol{X}_1 \succ \boldsymbol{X}_2 \succ \cdots \succ \boldsymbol{X}_t$ are monomials of $Mon(A^m)$.

Definition 1.4.14. *With the above notation, we say that*

(i) $lt(\boldsymbol{f}) := c_1\boldsymbol{X}_1$ *is the leading term of* $\boldsymbol{f}$*.*

(ii) $lc(\boldsymbol{f}) := c_1$ *is the leading coefficient of* $\boldsymbol{f}$*.*

(iii) $lm(\boldsymbol{f}) := \boldsymbol{X}_1$ *is the leading monomial of* $\boldsymbol{f}$*.*

For $\boldsymbol{f} = \boldsymbol{0}$ we define $lm(\boldsymbol{0}) = \boldsymbol{0}, lc(\boldsymbol{0}) = 0, lt(\boldsymbol{0}) = \boldsymbol{0}$, and if $\succeq$ is a monomial order on $Mon(A^m)$, then we define $\mathbf{X} \succ \mathbf{0}$ for any $\mathbf{X} \in Mon(A^m)$. So, we extend $\succeq$ to $Mon(A^m)\bigcup\{\mathbf{0}\}$.
The reduction process in A^m is defined as follows.

Definition 1.4.15. *Let F be a finite set of non-zero vectors of A^m, and let $\boldsymbol{f}, \boldsymbol{h} \in A^m$, we say that $\boldsymbol{f}$ reduces to $\boldsymbol{h}$ by F in one step, denoted $\boldsymbol{f} \xrightarrow{F} \boldsymbol{h}$, if there exist elements $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_t \in F$ and $r_1, \ldots, r_t \in R$ such that*

(i) $lm(\boldsymbol{f}_i)|lm(\boldsymbol{f})$, $1 \leq i \leq t$, *i.e.,* $ind(lm(\boldsymbol{f}_i)) = ind(lm(\boldsymbol{f}))$ *and there exists* $x^{\alpha_i} \in Mon(A)$ *such that* $\alpha_i + \exp(lm(\boldsymbol{f}_i)) = \exp(lm(\boldsymbol{f}))$*.*

(ii) $lc(\boldsymbol{f}) = r_1\sigma^{\alpha_1}(lc(\boldsymbol{f}_1))c_{\alpha_1,\boldsymbol{f}_1} + \cdots + r_t\sigma^{\alpha_t}(lc(\boldsymbol{f}_t))c_{\alpha_t,\boldsymbol{f}_t}$, *where* $c_{\alpha_i,\boldsymbol{f}_i} := c_{\alpha_i,\exp(lm(\boldsymbol{f}_i))}$*.*

(iii) $\boldsymbol{h} = \boldsymbol{f} - \sum_{i=1}^{t} r_i x^{\alpha_i}\boldsymbol{f}_i$*.*

We say that $\boldsymbol{f}$ reduces to $\boldsymbol{h}$ by F, denoted $\boldsymbol{f} \xrightarrow{F}_+ \boldsymbol{h}$, if and only if there exist vectors $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{t-1} \in A^m$ such that

$f\otimes_A \xrightarrow{Z} g$

$\boldsymbol{f}$ is reduced (also called minimal) w.r.t. F if $\boldsymbol{f} = \boldsymbol{0}$ or there is no one step reduction of $\boldsymbol{f}$ by F, i.e., one of the first two conditions of Definition 1.4.15 fails. Otherwise, we will say that $\boldsymbol{f}$ is reducible w.r.t. F. If $\boldsymbol{f} \xrightarrow{F}_+ \boldsymbol{h}$ and $\boldsymbol{h}$ is reduced w.r.t. F, then we say that $\boldsymbol{h}$ is a remainder for $\boldsymbol{f}$ w.r.t. F.

Theorem 1.4.16. *Let $F = \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_t\}$ be a set of non-zero vectors of A^m and $\boldsymbol{f} \in A^m$, then there exist polynomials $q_1, \ldots, q_t \in A$ and a reduced vector $\boldsymbol{h} \in A^m$ w.r.t. F such that $\boldsymbol{f} \xrightarrow{F}_+ \boldsymbol{h}$ and*

$$\boldsymbol{f} = q_1\boldsymbol{f}_1 + \cdots + q_t\boldsymbol{f}_t + \boldsymbol{h}$$

with

$$lm(\boldsymbol{f}) = \max\{lm(lm(q_1)lm(\boldsymbol{f}_1)), \ldots, lm(lm(q_t)lm(\boldsymbol{f}_t)), lm(\boldsymbol{h})\}.$$

In the last chapter we will implement the algorithm associated to the previous theorem. Next we have the definition of Gröbner basis for submodules of A^m.

Definition 1.4.17. *Let $M \neq 0$ be a submodule of A^m and let G be a non empty finite subset of non-zero vectors of M, we say that G is a Gröbner basis for M if each element $0 \neq \boldsymbol{f} \in M$ is reducible w.r.t. G.*

Theorem 1.4.18. *Let $M \neq 0$ be a submodule of A^m and let G be a finite subset of non-zero vectors of M. Then the following conditions are equivalent:*

(i) G is a Gröbner basis for M.

(ii) For any vector $\boldsymbol{f} \in A^m$,

$$\boldsymbol{f} \in M \text{ if and only if } \boldsymbol{f} \xrightarrow{G}_{+} \boldsymbol{0}.$$

In the last chapter will be implemented the Buchberger's algorithm for computing Gröbner basis.

1.4.3. Computing the module of syzygies of a submodule

Now we review how to compute the module of syzygies of a left ideal of A, and then, we generalize this to a submodule of A^m.

Definition 1.4.19. *Let $F := \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_s\} \subseteq A^m$ such that the least common multiple of $\{lm(\boldsymbol{g}_1), \ldots, lm(\boldsymbol{g}_s)\}$, denoted by $\boldsymbol{X}_F$, is non-zero. Let $\theta \in \mathbb{N}^n$, $\beta_i := \exp(lm(\boldsymbol{g}_i))$ and $\gamma_i \in \mathbb{N}^n$ such that $\gamma_i + \beta_i = \exp(\boldsymbol{X}_F)$, $1 \leq i \leq s$. $B_{F,\theta}$ will denote a finite set of generators of*

$$S_{F,\theta} := Syz_R[\sigma^{\gamma_1+\theta}(lc(\boldsymbol{g}_1))c_{\gamma_1+\theta,\beta_1} \ \cdots \ \sigma^{\gamma_s+\theta}(lc(\boldsymbol{g}_s))c_{\gamma_s+\theta,\beta_s})].$$

For $\theta = \boldsymbol{0} := (0, \ldots, 0)$, $S_{F,\theta}$ will be denoted by S_F and $B_{F,\theta}$ by B_F.

Let A^m be the left A-module of column vectors of length $m \geq 1$. Given I a left ideal of A, with $I = \langle f_1, \ldots f_s\}$, we may define the following A-homomorphism:

$$\phi : A^s \to I; \quad (h_1, \ldots, h_s)^T \mapsto \sum_{i=1}^{s} h_i f_i;$$

Note that ϕ is surjective and, therefore, $I \cong A^s / \ker(\phi)$.

Definition 1.4.20. *The kernel of ϕ is called the* ***syzygy module*** *of the matrix* $\begin{bmatrix} f_1 & \cdots & f_s \end{bmatrix}$. *It is denoted by $Syz(f_1, \dots, f_s)$. An element $(h_1, \dots, h_s)^T \in Syz(f_1, \dots, f_s)$ is called a* ***syzygy*** *of* $\begin{bmatrix} f_1 & \cdots & f_s \end{bmatrix}$ *and satisfies*

$$h_1 f_1 + \cdots + h_s f_s = 0.$$

Note that ϕ can be viewed as the matrix multiplication:

$$\phi(h_1, \dots, h_s) = \begin{bmatrix} h_1 & \cdots & h_s \end{bmatrix} \begin{bmatrix} f_1 \\ \vdots \\ f_s \end{bmatrix};$$

and $Syz(f_1, \dots f_s)$ as the set of all solutions $(h_1, \dots, h_s)^T \in A^s$ of the linear equation

$$\begin{bmatrix} h_1 & \cdots & h_s \end{bmatrix} \begin{bmatrix} f_1 \\ \vdots \\ f_s \end{bmatrix} = 0.$$

Since A is a left Noetherian ring, then $Syz(f_1, \dots, f_s)$ is a finitely generated left A-module. We will compute a system of generators for $Syz(f_1, \dots, f_s)$ for any $f_1, \dots, f_s \in A$. For this, we first compute a Gröbner basis $G = \{g_1, \dots, g_t\}$ for $I = \langle f_1, \dots, f_s \}$. Next, we obtain a set of generators for $Syz(g_1, \dots, g_t)$ and, finally, we will obtain a system of generators for $Syz(f_1, \dots, f_s)$ from one of $Syz(g_1, \dots, g_t)$.
So, let $G = \{g_1, \dots, g_t\}$ be a Gröbner basis for I, $F = \{g_{i_1}, \dots, g_{i_k}\} \subseteq G$ and $\boldsymbol{b} = (b_1, \dots, b_k) \in B_F$ (recall that B_F is a set of generators of $Syz_R(\sigma^{\gamma_j}(lc(g_{i_j}))c_{\gamma_j, \exp(g_{i_j})} \mid 1 \leq j \leq k))$; we know that $\sum_{j=1}^k b_j x^{\gamma_j} g_{i_j} \xrightarrow{G}_+ 0$ and hence there exist $h_1, \dots, h_s \in A$ such that $\sum_{j=1}^k b_j x^{\gamma_j} g_{i_j} = \sum_{i=1}^t h_i g_i$. For each $\boldsymbol{b} \in B_F$, we define

$$\boldsymbol{s_{bF}} := \sum_{j=1}^k b_j x^{\gamma_j} \boldsymbol{e}_{i_j} - (h_1, \dots, h_t) \in A^t;$$

then $\boldsymbol{s_{bF}} \in Syz(g_1, \dots, g_t)$: in fact,

$$\begin{aligned} \boldsymbol{s_{bF}} \begin{bmatrix} g_1 \\ \vdots \\ g_t \end{bmatrix} &= [\sum_{j=1}^k b_j x^{\gamma_j} \boldsymbol{e}_{i_j} - (h_1, \dots, h_t)] \begin{bmatrix} g_1 \\ \vdots \\ g_t \end{bmatrix} \\ &= \sum_{j=1}^k b_j x^{\gamma_j} g_{i_j} - \sum_{i=1}^t h_i g_i = 0. \end{aligned}$$

Definition 1.4.21. *Let $X_1, \dots, X_t \in Mon(A)$ and $J \subseteq \{1, \dots, t\}$. Let*

$$X_J := lcm\{X_j \mid j \in J\}.$$

We say that J is saturated with respect to $\{X_1, \dots, X_t\}$, if

$$X_j \mid X_J \Rightarrow j \in J,$$

for any $j \in \{1, \dots, t\}$. The saturation J' of J consists of all $j \in \{1, \dots, t\}$ such that $X_j \mid X_J$.

Theorem 1.4.22. *With the above notations, a generating set for* $Syz(g_1,\dots,g_t)$ *is*

$$S := \{\boldsymbol{s}_v^J \mid J \subseteq \{1,\dots,t\} \text{ is saturated w.r.t.} \{lm(g_1),\dots,lm(g_t)\}, 1 \leq v \leq l_J\},$$

where

$$\boldsymbol{s}_v^J := \sum_{j\in J} b_{vj}^J x^{\gamma_j} \boldsymbol{e}_j - (h_1^v,\dots,h_t^v),$$

with $\gamma_j \in \mathbb{N}^n$ *such that* $\gamma_j + \beta_j = \exp(X_J)$, $\beta_j = \exp(g_j)$ *for* $j \in J$, $B_J := \{\boldsymbol{b}_1^J,\dots,\boldsymbol{b}_{l_J}^J\}$ *a system of generators for* $S_J := Syz_R[\sigma^{\gamma_j}(lc(g_j))c_{\gamma_j,\beta_j} \mid j \in J]$, *and* $\boldsymbol{b}_v^J := (b_{vj}^J)_{j\in J}$ *for* $1 \leq v \leq l_J$.

As we saw in Theorem 1.4.8, there exist $H \in M_{s\times t}(A)$ and $Q \in M_{t\times s}(A)$ such that $G^T = H^T F^T$ and $F^T = Q^T G^T$, where $G := \begin{bmatrix} g_1 & \cdots & g_t \end{bmatrix}$, $F := \begin{bmatrix} f_1 & \cdots & f_s \end{bmatrix}$ and G is a Gröbner basis for I. By Theorem 1.4.22, we may compute a set of generators $\{\boldsymbol{s}_1,\dots,\boldsymbol{s}_l\}$ for $Syz(g_1,\dots,g_t)$. Thus, for each $1 \leq i \leq l$ we have that

$$\boldsymbol{s}_i H^T F^T = \boldsymbol{s}_i G^T = 0,$$

and therefore, $\langle \boldsymbol{s}_i H^T \mid 1 \leq i \leq l\rangle \subseteq Syz(f_1,\dots,f_s)$. Further,

$$\begin{bmatrix} I_s - Q^T H^T \end{bmatrix} \begin{bmatrix} f_1 \\ \vdots \\ f_s \end{bmatrix} = \begin{bmatrix} f_1 \\ \vdots \\ f_s \end{bmatrix} - Q^T H^T \begin{bmatrix} f_1 \\ \vdots \\ f_s \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix},$$

and thereby the rows $\boldsymbol{r}_1,\dots,\boldsymbol{r}_s$ of $I_s - Q^T H^T$ also belong to $Syz(f_1,\dots,f_s)$.

Theorem 1.4.23. *With the above notation, we have*

$$Syz(f_1,\dots,f_s) = \langle \boldsymbol{s}_1 H^T,\dots,\boldsymbol{s}_l H^T, \boldsymbol{r}_1,\dots,\boldsymbol{r}_s\rangle \leq A^s.$$

Now we can generalize the method described above for computing the syzygy module of a submodule $M = \langle \boldsymbol{f}_1,\dots,\boldsymbol{f}_s\rangle$ of A^m. Let $F := \begin{bmatrix} \boldsymbol{f}_1 & \cdots & \boldsymbol{f}_s \end{bmatrix}$, we recall that $Syz(M) := Syz(F)$ consists of column vectors $\boldsymbol{h} = \begin{pmatrix} h_1 & \cdots & h_s \end{pmatrix}^T \in A^s$ such that

$$h_1\boldsymbol{f}_1 + \cdots + h_s\boldsymbol{f}_s = \boldsymbol{0},$$

i.e., $\boldsymbol{h}^T F^T = \boldsymbol{0}$, and it is also the kernel of homomorphism $f : A^s \to M$, $\boldsymbol{e}_i \mapsto \boldsymbol{f}_i$, where $\{\boldsymbol{e}_i\}_{i=1}^s$ is the canonical basis of A^s. We note that $Syz(F)$ is a submodule of A^s and we can set a matrix with its generators, so sometimes we will refer to $Syz(F)$ as a matrix. We also will write

$$Syz(M) = Syz(F) = Syz(\{\boldsymbol{f}_1,\dots,\boldsymbol{f}_s\}). \tag{1-13}$$

The computation of $Syz(F)$ is done in two steps. First, we consider a Gröbner basis $G = \{\boldsymbol{g}_1,\dots,\boldsymbol{g}_t\}$ for M and we compute $Syz(G) := Syz(\{\boldsymbol{g}_1,\dots,\boldsymbol{g}_t\}) \leq A^t$, and then, we obtain a system of generators for $Syz(F)$ from one for $Syz(G)$. For $F = \{\boldsymbol{g}_{i_1},\dots,\boldsymbol{g}_{i_k}\} \subseteq G$ and

$(b_1,\dots,b_k)\in B_F$, with B_F a set of generators of $Syz_R(\sigma^{\gamma_j}(lc(\boldsymbol{g}_{i_j}))c_{\gamma_j,\exp(\boldsymbol{g}_{i_j})}\mid 1\leq j\leq k)$, we have that $\sum_{j=1}^k b_jx^{\gamma_j}\boldsymbol{g}_{i_j}\xrightarrow{G}_+ 0$, and hence, there exist $h_1,\dots,h_s\in A$ such that $\sum_{j=1}^k b_jx^{\gamma_j}\boldsymbol{g}_{i_j}=\sum_{i=1}^t h_i\boldsymbol{g}_i$. For each $\boldsymbol{b}\in B_F$, we define

$$\boldsymbol{s}_{\boldsymbol{b}F}:=\sum_{j=1}^k b_jx^{\gamma_j}\boldsymbol{e}_{i_j}-(h_1,\dots,h_t)\in A^t;$$

then $\boldsymbol{s}_{\boldsymbol{b}F}\in Syz(\boldsymbol{g}_1,\dots,\boldsymbol{g}_t)$: in fact,

$$\begin{aligned}\boldsymbol{s}_{\boldsymbol{b}F}\begin{bmatrix}\boldsymbol{g}_1\\ \vdots\\ \boldsymbol{g}_t\end{bmatrix}&=[\sum_{j=1}^k b_jx^{\gamma_j}\boldsymbol{e}_{i_j}-(h_1,\dots,h_t)]\begin{bmatrix}\boldsymbol{g}_1\\ \vdots\\ \boldsymbol{g}_t\end{bmatrix}\\&=\sum_{j=1}^k b_jx^{\gamma_j}\boldsymbol{g}_{i_j}-\sum_{i=1}^t h_i\boldsymbol{g}_i=0.\end{aligned}$$

Definition 1.4.24. *Let $\boldsymbol{X}_1,\dots,\boldsymbol{X}_t\in Mon(A^m)$ and $J\subseteq\{1,\dots,t\}$. Let*

$\boldsymbol{X}_J:=lcm\{\boldsymbol{X}_j\mid j\in J\}$.

We say that J is saturated with respect to $\{\boldsymbol{X}_1,\dots,\boldsymbol{X}_t\}$, if

$\boldsymbol{X}_j\mid\boldsymbol{X}_J\Rightarrow j\in J$,

for any $j\in\{1,\dots,t\}$. The saturation J' of J consists of all $j\in\{1,\dots,t\}$ such that $\boldsymbol{X}_j\mid\boldsymbol{X}_J$.

Theorem 1.4.25. *With the above notations, a generating set for $Syz(\boldsymbol{g}_1,\dots,\boldsymbol{g}_t)$ is*

$S:=\{\boldsymbol{s}_v^J\mid J\subseteq\{1,\dots,t\}$ *is saturated w.r.t.*$\{lm(\boldsymbol{g}_1),\dots,lm(\boldsymbol{g}_t)\},1\leq v\leq l_J\}$,

where

$$\boldsymbol{s}_v^J:=\sum_{j\in J}b_{vj}^Jx^{\gamma_j}\boldsymbol{e}_j-(h_1^v,\dots,h_t^v),$$

with $\gamma_j\in\mathbb{N}^n$ such that $\gamma_j+\beta_j=\exp(\boldsymbol{X}_J)$, $\beta_j=\exp(\boldsymbol{g}_j)$, $j\in J$, $B^J:=\{\boldsymbol{b}_1^J,\dots,\boldsymbol{b}_{l_J}^J\}$ is a system of generators for $S^J:=Syz_R[\sigma^{\gamma_j}(lc(\boldsymbol{g}_j))c_{\gamma_j,\beta_j}\mid j\in J]$, and $\boldsymbol{b}_v^J:=(b_{vj}^J)_{j\in J}$.

We return to the task of calculating a system of generators for $Syz(\boldsymbol{f}_1,\dots,\boldsymbol{f}_s)$, where $\{\boldsymbol{f}_1,\dots,\boldsymbol{f}_s\}$ is a collection of nonzero vectors, which non necessarily form a Gröbner basis for $M=\langle\boldsymbol{f}_1,\dots,\boldsymbol{f}_s\rangle$. From Theorem 1.4.8 (for modules), there exist $H\in M_{s\times t}(A)$ and $Q\in M_{t\times s}(A)$ such that $G^T=H^TF^T$ and $F^T=Q^TG^T$, where $G:=\begin{bmatrix}\boldsymbol{g}_1 & \cdots & \boldsymbol{g}_t\end{bmatrix}$, $F:=\begin{bmatrix}\boldsymbol{f}_1 & \cdots & \boldsymbol{f}_s\end{bmatrix}$ and G is a Gröbner basis for $\langle\boldsymbol{f}_1,\dots,\boldsymbol{f}_s\rangle$. By Theorem 1.4.25, we compute a set of generators $\{\boldsymbol{s}_1,\dots,\boldsymbol{s}_l\}$ for $Syz(\boldsymbol{g}_1,\dots,\boldsymbol{g}_t)$. Thus, for each $1\leq i\leq l$ we have

$$\boldsymbol{s}_iH^TF^T=\boldsymbol{s}_iG^T=0,$$

and therefore, $\langle \boldsymbol{s}_i H^T \mid 1 \leq i \leq l\rangle \subseteq Syz(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s)$. If $Syz(G) := Z(G) := \begin{bmatrix}\boldsymbol{s}_1 & \cdots & \boldsymbol{s}_l\end{bmatrix}$, then $Syz(\boldsymbol{g}_1, \ldots, \boldsymbol{g}_t)$ is the module generated by columns of $Z(G)$ and this last equation may be written as

$$Z(G)^T H^T F^T = Z(G)^T G^T = 0. \tag{1-14}$$

Further,

$$[I_s - Q^T H^T]\begin{bmatrix}\boldsymbol{f}_1\\ \vdots\\ \boldsymbol{f}_s\end{bmatrix} = \begin{bmatrix}\boldsymbol{f}_1\\ \vdots\\ \boldsymbol{f}_s\end{bmatrix} - Q^T H^T \begin{bmatrix}\boldsymbol{f}_1\\ \vdots\\ \boldsymbol{f}_s\end{bmatrix} = \begin{bmatrix}0\\ \vdots\\ 0\end{bmatrix},$$

and thereby the rows $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_s$ of $I_s - Q^T H^T$ also belong to $Syz(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s)$.

Theorem 1.4.26. *With the above notation, we have*

$$Syz(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s) = \langle \boldsymbol{s}_1 H^T, \ldots, \boldsymbol{s}_l H^T, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_s\rangle \leq A^s.$$

In a matrix notation, $Syz(F)$ coincides with the column module of the extended matrix

$$\begin{bmatrix}(Z(G)^T H^T)^T & (I_s - Q^T H^T)^T\end{bmatrix},$$

i.e.,

$$Syz(F) = \begin{bmatrix}(Z(G)^T H^T)^T & (I_s - Q^T H^T)^T\end{bmatrix} \tag{1-15}$$

1.4.4. Presentation of a module

Let $M = \langle \boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\rangle$ be a submodule of A^m, there exists a natural surjective homomorphism $\pi_M : A^s \longrightarrow M$ defined by $\pi_M(\boldsymbol{e}_i) := \boldsymbol{f}_i$, where $\{\boldsymbol{e}_i\}_{1\leq i\leq s}$ is the canonical basis of A^s. We have the isomorphism $\overline{\pi_M} : A^s/\ker(\pi_M) \cong M$, defined by $\overline{\pi_M}(\overline{\boldsymbol{e}_i}) := \boldsymbol{f}_i$, where $\overline{\boldsymbol{e}_i} := \boldsymbol{e}_i + \ker(\pi_M)$. Since A^s is a Noetherian A-module, $\ker(\pi_M)$ is also a finitely generated module, $\ker(\pi_M) := \langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{s_1}\rangle$, and hence, we have the exact sequence

$$A^{s_1} \xrightarrow{\delta_M} A^s \xrightarrow{\pi_M} M \longrightarrow 0, \tag{1-16}$$

with $\delta_M := l_M \circ \pi'_M$, where l_M is the inclusion of $\ker(\pi_M)$ in A^s and π'_M is the natural surjective homomorphism from A^{s_1} to $\ker(\pi_M)$. We note that $\ker(\pi_M) = Syz(M) = Syz(F)$, where $F = [\boldsymbol{f}_1 \cdots \boldsymbol{f}_s] \in M_{m\times s}(A)$

Definition 1.4.27. *It is said that $A^s/Syz(M)$ is a presentation of M. It is said also that the sequence (1-16) is a finite presentation of M, and M is a finitely presented module.*

Theorem 1.4.25 gives a method for computing a presentation of M when A is a bijective skew PBW extension. Moreover, let Δ_M be the matrix of δ_M in the canonical bases of A^{s_1} and A^s; since $Im(\delta_M) = \ker(\pi_M)$, then

$$\Delta_M = \begin{bmatrix}\boldsymbol{h}_1 & \cdots & \boldsymbol{h}_{s_1}\end{bmatrix} = \begin{bmatrix}h_{11} & \cdots & h_{1s_1}\\ \vdots & & \vdots\\ h_{s1} & \cdots & h_{ss_1}\end{bmatrix} \in M_{s\times s_1}(A),$$

and hence, the columns of Δ_M are the generators of $Syz(F)$. With the notation of Section 1.4.3, $\Delta_M = Z(F)$.

Definition 1.4.28. *With the previous notation, it is said that Δ_M is a matrix presentation of M.*

1.4.5. Free resolutions

In this subsection we present a theorem that let us to compute free resolutions for submodules of A^m. Let M be a submodule of A^m, we recall that a free resolution of M is an exact sequence of free modules and homomophisms

$$\cdots \xrightarrow{f_{r+1}} A^{s_r} \xrightarrow{f_r} A^{s_{r-1}} \xrightarrow{f_{r-1}} \cdots \xrightarrow{f_2} A^{s_1} \xrightarrow{f_1} A^{s_0} \xrightarrow{f_0} M \longrightarrow 0,$$

with $s_i \geq 0$ for each $i \geq 0$. We assume that $A^0 = 0$. r is the length of this sequence if $s_r \neq 0$ and $s_i = 0$ for $i \geq r+1$. The following theorem describes a simple procedure for constructing a free resolution of M (see [24] and [45]).

Theorem 1.4.29. *Let $M = \langle \boldsymbol{f}_1^{(0)}, \ldots, \boldsymbol{f}_{s_0}^{(0)} \rangle$ be a submodule of the free module A^m. Let F_0 be the matrix whose columns are $\boldsymbol{f}_1^{(0)}, \ldots, \boldsymbol{f}_{s_0}^{(0)}$, and for $i \geq 1$ let*

$$F_i := Syz(F_{i-1}) = [\boldsymbol{f}_1^{(i)} \cdots \boldsymbol{f}_{s_i}^{(i)}].$$

Then,

$$\cdots \xrightarrow{f_{r+1}} A^{s_r} \xrightarrow{f_r} A^{s_{r-1}} \xrightarrow{f_{r-1}} \cdots \xrightarrow{f_2} A^{s_1} \xrightarrow{f_1} A^{s_0} \xrightarrow{f_0} M \longrightarrow 0,$$

is a free resolution of M, where

$$f_i(\boldsymbol{e}_{j_i}^{(i)}) = \boldsymbol{f}_{j_i}^{(i)} = ((\boldsymbol{e}_{j_i}^{(i)})^T F_i^T)^T$$

and $\{\boldsymbol{e}_{j_i}^{(i)}\}_{1 \leq j_i \leq s_i}$ is the canonical basis of A^{s_i}.

2. Extended modules and rings for skew PBW extensions

The study of finitely generated projective modules induces the notions of $\mathcal{PSF}$, $\mathcal{PF}$, Hermite ($\mathcal{H}$), d-Hermite rings, and many other classes of interesting rings. In this chapter we will study another class of modules and rings useful for the investigation of projective modules. This special class arises when we try to generalize the famous Quillen-Suslin theorem about projective modules over polynomial rings with coefficients in $PIDs$ to a wider classes of coefficients (see [42]). In our context, of course, we are interested in investigating extended modules and rings for skew PBW extensions. Despite of some results of the present chapter can be proved for more general classes of skew PBW extensions, we will concentrate our attention in a particular type of these extensions: We will assume that R is a commutative ring and A will denote the skew PBW extension $A := R[x_1, \ldots, x_n; \sigma]$ for which σ is an automorphism of R, $x_ix_j = x_jx_i$ and $x_ir = \sigma(r)x_i$, for every $1 \leq i, j \leq n$. Observe that actually A is an Ore extension of R (see [64]). In some places we will assume some extra conditions on R. This second chapter, as well as the third and the last chapter, contain the main results of the thesis. We will preserve the notation used in the previous chapter (see Remark 1.3.2). $\langle X\rangle$ will denote the two-sided ideal of A generated by $x_1, \ldots, x_n$. Often we will used also the following notation for A, $A = \sigma(R)\langle X\rangle$. An element $p = c_0 + c_1X_1 + \cdots + c_tX_t \in A$, with $c_0, c_i \in R$ and $X_i \in Mon(A)$, $1 \leq i \leq t$, will be denoted also as $p = p(X)$. The elements of $Mon(A)$ will be represented by x^α or in capital letters, i.e., $x^\alpha = X$.
Recall that in this monograph all modules are left modules if nothing contrary is assumed. We will use the left notation for homomorphisms and row notation for matrix representation of homomorphisms between free modules.

2.1. Extended modules and rings

Definition 2.1.1. *Let $T \supseteq S$ be rings.*

(i) Let M be a T-module, M is extended from S if there exists an S-module M_0 such that $M \cong T \otimes_S M_0$. It also says that M is an extension of M_0 with respect to S.

(ii) $\mathfrak{M}(T)$ denotes the family of finitely generated T-modules, $\mathfrak{P}(T)$ the family of projective T-modules in $\mathfrak{M}(T)$ and $\mathfrak{P}^S(T)$ the family of modules in $\mathfrak{P}(T)$ extended from S.

(iii) The ring T is extended with respect to S, also called S-extended, if every finitely generated projective T-module is extended from S, i.e., $\mathfrak{P}(T) \subseteq \mathfrak{P}^S(T)$. For the extension

$A := R[x_1, \ldots, x_n; \sigma]$, we will say that A is $\mathcal{E}$ if A is R-extended.

We start presenting an elementary general proposition about extended modules and $\mathcal{PF}$ rings. A well known result due to Bass about projective modules is needed first.

Proposition 2.1.2 (Bass's Theorem). *Let I be a two-sided ideal of a ring R such that $I \subseteq Rad(R)$, and let P, Q be projective R-modules. Then, $P \cong Q$ if and only if $P/IP \cong Q/IQ$ as R/I-modules. In particular, P is R-free if and only if P/IP is R/I-free.*

Proof. See [14], Lemma 2.4. □

Proposition 2.1.3. *Let $T \supseteq S \supseteq R$ be rings and M a T-module.*

(i) If M is an extension of M_0 with respect to S and M_0 is an extension of L_0 with respect to R, then M is an extension of L_0 with respect to R.

(ii) If T is R-extended, then T is S-extended.

(iii) Let I be a proper two-sided ideal of T, with $S \cong T/I$. If T is $\mathcal{PF}$ then S is $\mathcal{PF}$.

(iv) Let J be a two-sided ideal of R such that $J \subseteq Rad(R)$. If R/J is $\mathcal{PF}$, then R is $\mathcal{PF}$.

Proof. (i) $M \cong T \otimes_S M_0$, $M_0 \cong S \otimes_R L_0$, then $M \cong T \otimes_S S \otimes_R L_0 \cong T \otimes_R L_0$.
(ii) $M \cong T \otimes_R M_0 \cong (T \otimes_S S) \otimes_R M_0 \cong T \otimes_S (S \otimes_R M_0)$.
(iii) Let $M \in \mathfrak{P}(S)$. Then, $M \oplus M' \cong S^r$ for some S-module M', therefore $(T \otimes_S M) \oplus M'' \cong T^r$, i.e., $T \otimes_S M \in \mathfrak{P}(T)$, so $T \otimes_S M$ is T-free, and hence $T \otimes_S M \cong T^\ell \cong T \otimes_S S^\ell$. Whence, $M \cong S \otimes_S M \cong (T/I \otimes_T T) \otimes_S M \cong T/I \otimes_T (T \otimes_S M) \cong T/I \otimes_T (T \otimes_S S^\ell) \cong (T/I \otimes_T T) \otimes_S S^\ell \cong S \otimes_S S^\ell \cong S^\ell$. Therefore, S is $\mathcal{PF}$.
(iv) Let $M \in \mathfrak{P}(R)$, then $R/J \otimes_R M \in \mathfrak{P}(R/J)$ so that

$$M/JM \cong R/J \otimes_R M \cong (R/J)^n \cong R/J \otimes_R R^n \cong R^n/JR^n.$$

From Proposition 2.1.2, $M \cong R^n$, and hence R is $\mathcal{PF}$. □

2.2. Extended rings and Ore extensions

From now on in the present chapter (except in the last section) we will assume that R is a commutative ring and A will denote the Ore extension $A := R[x_1, \ldots, x_n; \sigma]$ for which σ is an automorphism of R, $x_i x_j = x_j x_i$ and $x_i r = \sigma(r) x_i$, for every $1 \leq i, j \leq n$.

Proposition 2.2.1. *Let M be an A-module. Then,*

(i) If M is free, then M is extended from R.

(ii) If M is an extension of M_0 with respect to R, then

$$M_0 \cong M/\langle X \rangle M. \tag{2-1}$$

Moreover, if M is finitely generated (projective, stably free) as A-module, then M_0 is finitely generated (projective, stably free) as R-module.

Proof. (i) $M \cong A^{(Y)}$, then $M \cong A \otimes_R R^{(Y)}$ (note that this property is still valid for any couple of rings $A \supseteq R$).
(ii) First recall that since A is a quasi-commutative skew PBW extension, then $A/\langle X\rangle \cong R$ (see Remark 1.3.6). If $M \cong A \otimes_R M_0$ then $A/\langle X\rangle \otimes_A M \cong A/\langle X\rangle \otimes_A A \otimes_R M_0$, i.e., $M/\langle X\rangle M \cong A/\langle X\rangle \otimes_R M_0 \cong R \otimes_R M_0 \cong M_0$.
Let $M = \langle z_1, \ldots, z_t\rangle$ and $w \in M_0$, then $w = \overline{z}$ with $z \in M$; there exist $p_1(X), \ldots, p_t(X) \in A$ such that $w = \overline{z} = \overline{p_1(X)z_1 + \cdots + p_t(X)z_t} = p_{01}\overline{z_1} + \cdots + p_{0t}\overline{z_t}$, where p_{0i} is the independent term of $p_i(X)$, $1 \leq i \leq t$. Hence, $M_0 = \langle \overline{z_1}, \ldots, \overline{z_t}\rangle$.
If M is projective, then $M \oplus M' = A^{(Y)}$, and $A/\langle X\rangle \otimes_A (M \oplus M') \cong A/\langle X\rangle \otimes_A A^{(Y)}$, i.e., $M_0 \oplus M'/\langle X\rangle M' \cong R^{(Y)}$.
If M is stably free, then $M \oplus A^r = A^s$, so applying $A/\langle X\rangle \otimes_A$ we get $M_0 \oplus R^r \cong R^s$. □

We can give a matrix description of extended rings. Firstly we recall the definition of square similar matrices.

Definition 2.2.2. *Let S be a ring and $F, G \in M_s(S)$, it is said that F and G are similar if there exists $P \in G_s(S)$ such that $F = PGP^{-1}$. In particular, let $F(X)$ be a square matrix over A of size $s \times s$ and $F(0)$ the matrix over R obtained from $F(X)$ replacing all the variables $x_1, \ldots, x_n$ by 0,*

$$F(X) \sim F(0) \Leftrightarrow F(0) = P(X)F(X)P(X)^{-1}, \text{ for some } P(X) \in GL_s(A). \tag{2-2}$$

Theorem 2.2.3. *Let M be a finitely generated projective A-module and $F(X) \in M_s(A)$ be an idempotent matrix such that $M = \langle F(X)\rangle$, where $\langle F(X)\rangle$ is the A-module generated by the rows of $F(X)$.*

(i) If $F(X) \sim F(0)$, then M is extended from R.

(ii) If M is extended from R, then there exists a non zero matrix $P(X) \in M_s(A)$ such that $P(X)F(0) = F(X)P(X)$.

(iii) If A is such that for every $s \geq 1$, given an idempotent matrix $F(X) \in M_s(A)$, $F(X) \sim F(0)$, then A is $\mathcal{E}$.

(iv) If A is $\mathcal{E}$, then for every $s \geq 1$, given an idempotent matrix $F(X) \in M_s(A)$, there exists a non zero matrix $P(X) \in M_s(A)$ such that $P(X)F(X) = F(0)P(X)$.

Proof. (i) There exists $P(X) \in GL_s(A)$ such that $P(X)F(X)P(X)^{-1} = F(0)$. Since A is quasi-commutative, $F(0) \in M_s(R)$ is idempotent. Let $M_0 := \langle F(0)\rangle$ the R-module generated by the rows of $F(0)$, then M_0 is a finitely generated projective R-module. We will prove that $\langle F(X)\rangle \cong A \otimes_R M_0$, i.e., M is extended from R. $F(X), P(X)$ define A-endomorphisms of A^s, with $P(X)$ bijective, and $F(0)$ define a R-endomorphism of R^s. Let $G(X) := i_A \otimes_R F(0)$, then the following diagram

$$\begin{array}{ccc}
A^s \cong A \otimes_R R^s & \xrightarrow{G(X)} & A \otimes_R R^s \cong A^s \\
{\scriptstyle P(X)}\downarrow & & \downarrow{\scriptstyle P(X)} \\
A^s & \xrightarrow{F(X)} & A^s.
\end{array}$$

is commutative since $P(X)F(X)P(X)^{-1} = F(0)$ and the matrix of $G(X)$ in the canonical basis of A^s coincides with $F(0)$. From this we conclude that $\langle F(X)\rangle = Im(F(X)) \cong Im(G(X)) \cong Im(i_A) \otimes Im(F(0)) = A \otimes_R M_0$.
(ii) We have $M \cong A \otimes_R M_0$, for some finitely generated projective R-module M_0, but by Proposition 2.2.1, $M_0 \cong M/\langle X\rangle M = \langle F(X)\rangle/\langle X\rangle\langle F(X)\rangle = \langle F(0)\rangle$, so M_0 is generated by s elements. Thus, we have $Im(F(X)) = \langle F(X)\rangle \cong A \otimes_R \langle F(0)\rangle = Im(G(X))$, where $F(X)$ and $G(X) = F(0)$ are the idempotent endomorphisms of A^s as in (i). Let $H(X) : Im(F(X)) \to Im(F(0))$ be an isomorphism. We have

$$A^s = Im(F(X)) \oplus \ker(F(X)) = Im(F(0)) \oplus \ker(F(0)).$$

Let $T(X)$ be any A-homomorphism from $\ker(F(X))$ to $\ker(F(0))$, for example, $\boldsymbol{w}(X)T(X) := \boldsymbol{w}(0)$, with $\boldsymbol{w}(X) \in \ker(F(X))$. We have the following diagram

$$\begin{array}{ccc} A^s & \xrightarrow{F(X)} & A^s \\ {\scriptstyle P(X)}\downarrow & & \downarrow{\scriptstyle P(X)} \\ A^s & \xrightarrow{F(0)} & A^s \end{array}$$

where $P(X)$ is the A-homomorphism defined by $P(X) := H(X) \oplus T(X)$. Note that the diagram is commutative: If $\boldsymbol{v}(X) = \boldsymbol{u}(X)F(X) + \boldsymbol{w}(X)$, with $\boldsymbol{u}(X) \in A^s$ and $\boldsymbol{w}(X) \in \ker(F(X))$, then

$$\boldsymbol{v}(X)F(X)P(X) = \boldsymbol{u}(X)F(X)^2P(X) + \boldsymbol{w}(X)F(X)P(X) = \boldsymbol{u}(X)F(X)H(X);$$

on the other side,

$$\begin{gathered} \boldsymbol{v}(X)P(X)F(0) = [\boldsymbol{u}(X)F(X)H(X) + \boldsymbol{w}(X)T(X)]F(0) = \\ \boldsymbol{u}(X)F(X)H(X)F(0) + \boldsymbol{w}(X)T(X)F(0) = \boldsymbol{u}(X)F(X)H(X), \end{gathered}$$

where the last equality follows from the fact that $\boldsymbol{u}(X)F(X)H(X) \in Im(F(0))$ and $\boldsymbol{w}(X)T(X) \in \ker(F(0))$.
This proves that $P(X)F(0) = F(X)P(X)$. If $F(X) \neq 0$, then $H(X) \neq 0$ and hence $P(X) \neq 0$; if $F(X) = 0$, then $F(0) = 0$, $H(X) = 0$, $\ker(F(X)) = A^s = \ker(F(0))$ and we can take $T(X) = P(X) = i_{A^s}$.
(iii) is a direct consequence of (i) and (iv) follows from (ii). □

Remark 2.2.4. In the proof of (ii) we observed that

$$\ker(F(X)) \cong A^s/Im(F(X)) \text{ and } \ker(F(0)) \cong A^s/Im(F(0))$$

are finitely presented modules with $Im(F(X)) \cong Im(F(0))$. If there exists at least one surjective homomorphism $T(X)$ from $\ker(F(X))$ to $\ker(F(0))$ and A is left Noetherian, then $P(X)$ is surjective, and hence bijective, i.e., in this situation $F(X) \sim F(0)$.

The following results relate the conditions $\mathcal{E}$ and $\mathcal{PF}$ for the extension A.

Proposition 2.2.5. *Suppose that R is $\mathcal{PF}$. A is $\mathcal{E}$ if and only if A is $\mathcal{PF}$.*

Proof. $\Rightarrow$): Let M be a f.g. projective A-module, then $M \cong A \otimes_R M_0$, where M_0 is a f.g. projective R-module (Proposition 2.2.1). But since R is $\mathcal{PF}$, then M_0 is R-free and hence M is A-free.
$\Leftarrow$): If M is a f.g. projective left A-module, then M is A-free, then by Proposition 2.2.1, M is extended from R. □

Remark 2.2.6. Note that the previous proposition is valid for any couple of rings $A \supseteq R$.

Proposition 2.2.7. *If A is $\mathcal{PF}$, then R is $\mathcal{PF}$.*

Proof. We know that $A/\langle X\rangle \cong R$, so the result follows form Proposition 2.1.3. □

Corollary 2.2.8. *A is $\mathcal{PF}$ if and only if R is $\mathcal{PF}$ and A is $\mathcal{E}$*

Proof. This is direct consequence of Propositions 2.2.5 and 2.2.7. □

Corollary 2.2.9. *Let R be a Noetherian, regular and $\mathcal{PSF}$ ring. Then, A is $\mathcal{H}$ if and only if R is $\mathcal{PF}$ and A is $\mathcal{E}$.*

Proof. This follows Theorem 1.3.10 and Corollary 2.2.8. □

Remark 2.2.10. Let $A := R[x; \sigma]$ be the skew polynomial ring over $R = K[y]$, where K is a field and $\sigma(y) := y + 1$.
(i) From [64] 12.2.11 we know that A is not $\mathcal{E}$ with respect to R, and hence, from numeral (ii) in Proposition 2.1.3, we conclude that A is not $\mathcal{E}$ with respect to K. But precisely observe that $A = K[t; i_K][x; \sigma]$ is an Ore extension such that the σ's are different and $tx \neq xt$. Thus, the conditions we are assuming in this chapter about the commutativity of the variables and the restriction to only one automorphism for the ring of coefficients are more than important.
(ii) On the other hand, since R is a commutative principal ideal domain (PID) then R is $\mathcal{PF}$, therefore, by Corollary 2.2.8, A is not $\mathcal{PF}$. This means that in Theorem 2.5.3 below we can not weak the condition on K to be a commutative PID.
(iii) In addition, observe that R is a commutative Noetherian regular ring with finite Krull dimension and however A is not $\mathcal{E}$, so the Bass-Quillen conjecture (see [42]) in the case of our Ore extensions conduces to Quillen-Suslin Theorem 2.6.1.
(iv) Finally, this example also shows that although R is $\mathcal{H}$, $R[x; \sigma]$ is not $\mathcal{H}$. In fact, since R is $\mathcal{PF}$, we conclude that R is $\mathcal{PSF}$, so the claimed follows from Corollary 2.2.9. Thus, the Hermite conjecture for Ore extensions fails (see [42]).

2.3. Varserstein's theorem

Let R be a commutative ring, the Vaserstein's theorem in commutative algebra says that if $F(x_1, \dots, x_n) \in M_{r\times s}(R[x_1, \dots, x_n])$, then, $F(x_1, \dots, x_n) \sim F(0)$ if and only if for every $\mathfrak{m} \in \operatorname{Max}(R)$, $\overline{F(x_1, \dots, x_n)} \sim \overline{F(0)}$, where $\overline{F(x_1, \dots, x_n)}$ represents the image of $F(x_1, \dots, x_n)$ in $R_\mathfrak{m}[x_1, \dots, x_n]$ and $\sim$ denotes the relation of equivalence between matrices, i.e.,

$$F(X) = P(X)F(0)Q(X),$$

with $P(X) \in GL_r(R[x_1, \ldots, x_n])$ and $Q(X) \in GL_s(R[x_1, \ldots, x_n])$. In this section we extends this theorem to extensions of type $A := R[x_1, \ldots, x_n; \sigma]$.
Recall (Lemma 1.3.11) that if S is a multiplicative system of R and $\sigma(S) \subseteq S$, then $S^{-1}A$ exists and

$$S^{-1}A \cong (S^{-1}R)[x_1, \cdots x_n; \overline{\sigma}], \text{ with } \overline{\sigma}(\tfrac{r}{s}) := \tfrac{\sigma(r)}{\sigma(s)}.$$

In particular, if $\mathfrak{m} \in \mathrm{Max}(R)$ and $S := R - \mathfrak{m}$, we write

$$A_{\mathfrak{m}} := S^{-1}A \cong R_{\mathfrak{m}}[x_1, \ldots, x_n; \overline{\sigma}], \text{ where } \sigma \text{ satisfies } \sigma(s) \notin \mathfrak{m} \text{ for any } s \notin \mathfrak{m}.$$

From now on in the present chapter we will assume that σ satisfies the following condition:

$$\clubsuit\text{: Given } \mathfrak{m} \in \mathrm{Max}(R), \text{ if } s \notin \mathfrak{m}, \text{ then } \sigma(s) \notin \mathfrak{m}.$$

Some preliminary results are needed for the main theorem.

Proposition 2.3.1. *Let B be a ring and σ an endomorphism of B. Then,*

(i) For every $r \geq 1$, $M_r(B[x_1, \ldots, x_n; \sigma]) \cong M_r(B)[x_1, \ldots, x_n; \sigma]$.

(ii) If $\sigma(Z(B)) \subseteq Z(B)$ and $s \in Z(B)$, then

$$\begin{aligned} \phi : B[x_1, \ldots, x_n; \sigma] &\to B[x_1, \ldots, x_n; \sigma] \\ p(x_1, \ldots, x_n) &\mapsto p(sx_1, \ldots, sx_n) \end{aligned}$$

is a ring homomorphism.

(iii) φ defined as

$$\begin{aligned} \varphi : B[x_1, \ldots, x_n; \sigma] &\to B[x_1, \ldots, x_n; y_1, \ldots, y_n; \sigma] \ , \\ \varphi(p(x_1, \ldots, x_n)) &:= p(x_1 + y_1, \ldots, x_n + y_n) \end{aligned}$$

is a ring homomorphism.

Proof. (i) Using an inductive argument we only need to show that $M_r(B[x_1; \sigma]) \cong M_r(B)[x_1; \sigma]$. If we define $\sigma(F) := [\sigma(f_{ij})]$, with $F := [f_{ij}] \in M_r(B)$, then the claimed isomorphism is given by

$$F^{(0)} + F^{(1)}x_1 + \cdots + F^{(t)}x_1^t \mapsto [\textstyle\sum_{k=0}^{t} f_{ij}^{(k)} x_1^k].$$

(ii) It is clear that ϕ is additive and $\phi(1) = 1$. So, we have to show that $\phi(ax^\alpha bx^\beta) = \phi(ax^\alpha)\phi(bx^\beta)$ for every $a, b \in B$ and $\alpha, \beta \in \mathbb{N}^n$. Since $\sigma^k(s) \in Z(B)$ for every $k \geq 0$, then

$$\begin{aligned} \phi(ax^\alpha bx^\beta) &= \phi(a\sigma^\alpha(b)x^{\alpha+\beta}) = a\sigma^\alpha(b)(sx_1)^{\alpha_1+\beta_1} \cdots (sx_n)^{\alpha_n+\beta_n} \\ &= a\sigma^\alpha(b)s\sigma(s)\sigma^2(s) \cdots \sigma^{\alpha_1+\alpha_2+\cdots+\alpha_n+\beta_1+\beta_2+\cdots+\beta_n-1}(s)x^{\alpha+\beta}; \\ \phi(ax^\alpha)\phi(bx^\beta) &= a(sx_1)^{\alpha_1} \cdots (sx_n)^{\alpha_n} b(sx_1)^{\beta_1} \cdots (sx_n)^{\beta_n} \\ &= a\sigma^\alpha(b)s\sigma(s)\sigma^2(s) \cdots \sigma^{\alpha_1+\alpha_2+\cdots+\alpha_n+\beta_1+\beta_2+\cdots+\beta_n-1}(s)x^{\alpha+\beta}. \end{aligned}$$

(iii) Obviously φ is additive and $\varphi(1)=1$. Only rest to show that $\varphi(ax^\alpha bx^\beta)=\varphi(ax^\alpha)\varphi(bx^\beta)$ for every $a,b\in B$ and $\alpha,\beta\in\mathbb{N}^n$.

$$\begin{aligned}\varphi(ax^\alpha bx^\beta)&=\varphi(a\sigma^\alpha(b)x^{\alpha+\beta})=a\sigma^\alpha(b)(x_1+y_1)^{\alpha_1+\beta_1}\cdots(x_n+y_n)^{\alpha_n+\beta_n};\\ \varphi(ax^\alpha)\varphi(bx^\beta)&=a(x_1+y_1)^{\alpha_1}\cdots(x_n+y_n)^{\alpha_n}b(x_1+y_1)^{\beta_1}\cdots(x_n+y_n)^{\beta_n}\\ &=a\sigma^\alpha(b)(x_1+y_1)^{\alpha_1+\beta_1}\cdots(x_n+y_n)^{\alpha_n+\beta_n}.\end{aligned}$$

□

Lemma 2.3.2. *Let B be a ring, $S\subset Z(B)$ a multiplicative system of B. Let $A:=B[x_1,\dots,x_n;\sigma]$ be an Ore extension such that $\sigma(Z(B))\subseteq Z(B)$. Given the matrices $F(X)\in M_{r\times s}(A)$, $G(X)\in M_{s\times t}(A)$ and $H(X)\in M_{r\times t}(A)$, let $\overline{L(X)}$ be the image of the matrix $L(X)$ corresponding to the canonical homomorphism*

$$B[x_1,\dots,x_n;\sigma]\to(S^{-1}B)[x_1,\dots,x_n;\overline{\sigma}],\quad \overline{\sigma}(\tfrac{r}{s}):=\tfrac{\sigma(r)}{\sigma(s)}.$$

Suppose that $\overline{F(X)}\,\overline{G(X)}=\overline{H(X)}$ and $F(0)G(0)=H(0)$. Then, there exists $s\in S$ such that $F(sX)G(sX)=H(sX)$, where $L(sX):=L(sx_1,\dots,sx_n)$.

Proof. Let $D(X):=F(X)G(X)-H(X)$; since $F(0)G(0)-H(0)=0$ then

$$D(X)=D^{(1)}x^{\alpha_1}+D^{(2)}x^{\alpha_2}+\cdots+D^{(\ell)}x^{\alpha_\ell},$$

with $D^{(k)}\in M_{r\times t}(R)$, and $x^{\alpha_k}:=x_1^{\alpha_{k1}}\cdots x_n^{\alpha_{kn}}$, where $\alpha_{k1}+\cdots+\alpha_{kn}>0$ for every $1\le k\le\ell$. From $\overline{D(X)}=\overline{F(X)G(X)-H(X)}=\overline{F(X)}\,\overline{G(X)}-\overline{H(X)}=\overline{0}$ we conclude that

$$\overline{D^{(1)}}x^{\alpha_1}+\overline{D^{(2)}}x^{\alpha_1}+\cdots+\overline{D^{(\ell)}}x^{\alpha_\ell}=\overline{0}.$$

Then, each entry $d_{ij}^{(k)}$ of the matrix $D^{(k)}$ is such that $\frac{d_{ij}^{(k)}}{1}=\frac{0}{1}$ in $S^{-1}R$, so we find $s_{ij}^{(k)}\in S$ such that $s_{ij}^{(k)}d_{ij}^{(k)}=0$. Let $s:=\prod_{i,j,k}s_{ij}^{(k)}$, then $s\in Z(B)$ and $D^{(k)}s=0$ for each $k=1,\dots,\ell$. Thus, using Lemma 2.3.1, we get

$$F(sX)G(sX)-H(sX)=D(sX)=$$
$$D^{(1)}s\sigma(s)\sigma^2(s)\cdots\sigma^{\alpha_{11}+\cdots+\alpha_{1n}-1}(s)x^{\alpha_1}+\cdots+D^{(\ell)}s\sigma(s)\sigma^2(s)\cdots\sigma^{\alpha_{11}+\cdots+\alpha_{ln}-1}(s)x^{\alpha_\ell}=0.$$

□

Theorem 2.3.3 (Vaserstein's theorem). *Let R be a commutative ring and $A:=R[x_1,\dots,x_n;\sigma]$. Then, $F(X)\in M_{r\times s}(A)$ is equivalent to $F(0)$ if and only if $F(X)$ is locally equivalent to $F(0)$ for every $\mathfrak{m}\in\operatorname{Max}R$.*

Proof. $\Rightarrow$): Evident.
$\Leftarrow$): We denote I the set of elements $a\in R$ with the following property:

Given $f=(f_1,\dots,f_n),g=(g_1,\dots,g_2)\in A^n$ with $f-g\in a\,A^n$, then $F(f)\sim F(g)$.

$F(f)$ represents the evaluation $x_i \mapsto f_i$, $1 \leq i \leq n$, on the matrix $F(X)$. We claim that I is an ideal of R. In fact, let $a, b \in I$ and $f - g \in (a-b)A^n$, then $f - g = (a-b)h$, with $h \in A^n$, so $f - (g - bh) = ah \in a\,A^n$, and hence $F(f) \sim F(g - bh)$. But $g - (g - bh) = bh \in b\,A^n$, so $F(g - bh) \sim F(g)$, whence, $a - b \in I$. Let $r \in R$, $a \in I$ and $f - g \in ar\,A^n \subseteq a\,A^n$, therefore $F(f) \sim F(g)$, and this means that $ar \in I$.
If we show that $I = R$, then for every $f, g \in A^n$, $F(f) \sim F(g)$, in particular, if $f = (x_1, \ldots, x_n)$ and $g = (0, \ldots, 0)$, we obtain $F(X) \sim F(0)$. Let $\mathfrak{m} \in \operatorname{Max} R$; there exists $\overline{G(X)} \in \mathrm{GL}_r(R_\mathfrak{m}[x_1, \ldots, x_n; \overline{\sigma}])$ and $\overline{H(X)} \in \mathrm{GL}_s(R_\mathfrak{m}[x_1, \ldots, x_n; \overline{\sigma}])$ such that

$$\overline{F(X)} = \overline{G(X)}\,\overline{F(0)}\,\overline{H(X)}.$$

Introducing the Ore extension $R_\mathfrak{m}[x_1, \ldots, x_n; y_1, \ldots, y_n; \overline{\sigma}]$, i.e., $x_i x_j = x_j x_i$, $x_i y_j = y_j x_i$ and $y_i y_j = y_j y_i$ for $1 \leq i, j \leq n$, and $y_i \frac{r}{s} := \overline{\sigma}(\frac{r}{s}) y_i = \frac{\sigma(r)}{\sigma(s)} y_i$, we obtain, from Proposition 2.3.1, that

$$\overline{F(X+Y)} = \overline{G(X+Y)}\,\overline{F(0)}\,\overline{H(X+Y)}, \text{ where } Y := (y_1, \ldots, y_n). \tag{2-3}$$

Since $\overline{F(0)} = \overline{G(X)}^{-1}\overline{F(X)}\;\overline{H(X)}^{-1}$, we get

$$\overline{F(X+Y)} = \overline{G(X+Y)}\;\overline{G(X)}^{-1}\overline{F(X)}\;\overline{H(X)}^{-1}\,\overline{H(X+Y)}.$$

Denote $G^* := \overline{G(X+Y)}\;\overline{G(X)}^{-1}$ and $H^* := \overline{H(X)}^{-1}\,\overline{H(X+Y)}$. Observe that G^* has the form

$$\overline{G_0(X)} + \overline{G_1(X)} y^{\alpha_1} + \cdots + \overline{G_\ell(X)} y^{\alpha_\ell},$$

with $\overline{G_i(X)} \in M_r(R_\mathfrak{m}[x_1, \ldots, x_n; \overline{\sigma}])$, for every $i = 1, \ldots, \ell$, where $\overline{G_0(X)}$ is the identity matrix, and $y^{\alpha_i} := y_1^{\alpha_{i1}} \cdots y_n^{\alpha_{in}}$, for every $1 \leq i \leq \ell$. Moreover,

$$\overline{G_i(X)} y^{\alpha_i} = \overline{E_0} y^{\alpha_i} + \cdots + \overline{E_{i_j}} y^{\alpha_i} x^{\beta_{i_j}}, \text{ where } \overline{E_k} \in M_r(R_\mathfrak{m}), \text{ for } 0 \leq k \leq i_j. \tag{2-4}$$

Taking a common denominator we find $s' \in S$ and matrices $D_k \in M_r(R)$ such that

$$\overline{E_k} = \frac{D_k}{s'} = \frac{D_k s' \sigma(s') \sigma^2(s') \cdots \sigma^{\alpha_{i1} + \cdots + \alpha_{in} - 1}(s')}{s' \sigma(s') \sigma^2(s') \cdots \sigma^{\alpha_{i1} + \cdots + \alpha_{in} - 1}(s')},$$

so we can assume that $\overline{E_k} = \frac{D_k}{s' \sigma(s') \sigma^2(s') \cdots \sigma^{\alpha_{i1} + \cdots + \alpha_{in} - 1}(s')}$
Hence, replacing Y by $s'Y$ we get that $\overline{G(X+s'Y)}\,\overline{G(X)}^{-1}$ is the image of a matrix with entries over $R[x_1, \ldots, x_n; y_1, \ldots, y_n; \sigma]$. In a similar way we can do with $\overline{H(X)}^{-1}\,\overline{H(X+Y)}$. Thus, we can suppose that

$$\overline{G(X+s'Y)}\,\overline{G(X)}^{-1} \quad \text{and} \quad \overline{H(X)}^{-1}\,\overline{H(X+s'Y)}$$

are images of invertible matrices

$$\Gamma(X, Y) \quad \text{and} \quad \Delta(X, Y),$$

respectively, with entries in $R[x_1,\dots,x_n;y_1,\dots,y_n;\sigma]$, where $\Gamma(X,0)$ and $\Delta(X,0)$ are identities matrices.
On $R_{\mathfrak{m}}[x_1,\dots,x_n;y_1,\dots,y_n;\overline{\sigma}]$, we have the equation

$$\overline{F(X+s'Y)} = \overline{G(X+s'Y)}\,\overline{G(X)}^{-1}\overline{F(X)}\,\overline{H(X)}^{-1}\,\overline{H(X+s'Y)},$$

and on $R[x_1,\dots,x_n;\sigma]$,

$$F(X) = \Gamma(X,0)F(X)\Delta(X,0).$$

Taking $B := R[x_1,\dots,x_n;\sigma]$ in Lemma 2.3.2, there exists $s'' \in R - \mathfrak{m}$ such that for $s := s's''$, we have the equation

$$F(X+sY) = \Gamma(X,s''Y)F(X)\Delta(X,s''Y)$$

in the Ore extension $R[x_1,\dots,x_n;y_1,\dots,y_n;\sigma]$. Now if $f,g,h \in A^n$ are such that $f-g = sh$, we have

$$F(f) = F(g+sh) = \Gamma(g,s''h)F(g)\Delta(g,s''h),$$

where $\Gamma(g,s''h)$ and $\Delta(g,s''h)$ are invertible; then $F(f) \sim F(g)$ and so $s \in I$. We have showed that for every $\mathfrak{m} \in \operatorname{Max} R$ there exists $s \in I$ with $s \notin \mathfrak{m}$, i.e., $I = R$. □

2.4. Quillen's patching theorem

Now we will study another classical result of commutative algebra for the Ore extensions of type $A := R[x_1,\dots,x_n;\sigma]$, with R commutative: the famous Quillen's patching theorem. For this we will adapt the method studied in [41].
With the notation of the previous section, note that $A_{\mathfrak{m}}$ is a right A-module and if M is a left A-module, then we denote

$$M_{\mathfrak{m}} := A_{\mathfrak{m}} \otimes_A M = R_{\mathfrak{m}}[x_1,\dots,x_n;\overline{\sigma}] \otimes_A M.$$

If N is a right R-module, then we denote

$$N[x_1,\dots,x_n;\sigma] := N \otimes_R A.$$

Theorem 2.4.1 (**Quillen's patching theorem**). *Let R be a commutative ring and $A := R[x_1,\dots,x_n;\sigma]$. Let M be a finitely presented A-module. M is extended from R if and only if $M_{\mathfrak{m}}$ is extended from $R_{\mathfrak{m}}$, for every $\mathfrak{m} \in \operatorname{Max}(R)$.*

Proof. There exists an exact sequence of A-modules

$$A^p \xrightarrow{\beta_1} A^q \xrightarrow{\alpha_1} M \longrightarrow 0. \tag{2-5}$$

Tensoring by $A/\langle X\rangle$ we obtain the exact sequence of R-modules

$$R^p \xrightarrow{\overline{\beta}_1} R^q \xrightarrow{\overline{\alpha}_1} M/\langle X\rangle M \longrightarrow 0. \tag{2-6}$$

If $B \in M_{p\times q}(A)$ is the matrix of β_1 with respect to the canonical basis, then $B(0)$ is the matrix of $\overline{\beta}_1$. From (2-6) we get an exact sequence of A-modules, where $N := M/\langle X\rangle M$:

$$R^p[x_1,\dots,x_n;\sigma] \xrightarrow{\overline{\beta}_1[X]} R^q[x_1,\dots,x_n;\sigma] \xrightarrow{\overline{\alpha}_1[X]} N[x_1,\dots,x_n;\sigma] \to 0. \tag{2-7}$$

Note that $\overline{\beta}_1[X] := \overline{\beta_1} \otimes i_A$ and $\overline{\alpha}_1[X] := \overline{\alpha_1} \otimes i_A$. The sequence (2-7) can be identified with the exact sequence of A-modules

$$A^p \xrightarrow{\beta_2} A^q \xrightarrow{\alpha_2} N[x_1,\dots,x_n;\sigma] \longrightarrow 0, \tag{2-8}$$

where β_2 is described by the matrix $B(0)$. From Corollary 1.2.3, we have $M \cong N[x_1,\dots,x_n;\sigma]$ if and only if the $2(p+q)\times(2q)$-matrices

$$F := \left[\begin{array}{c|c} B & 0 \\ \hline 0 & I_q \\ \hline \multicolumn{2}{c}{0} \end{array}\right] \qquad \text{and} \qquad G := \left[\begin{array}{c|c} \multicolumn{2}{c}{0} \\ \hline I_q & 0 \\ \hline 0 & B(0) \end{array}\right]$$

are equivalent. Note that G is equivalent to $F(0)$ (permuting rows and columns). Therefore, by Theorem 2.3.3, $M \cong N[x_1,\dots,x_n;\sigma]$ if and only if F and $F(0)$ are locally equivalent for every $\mathfrak{m} \in \mathrm{Max}(R)$. Since the exact sequences (2-5) and (2-8) are consistent with respect to the localization by $\mathfrak{m}$, we get that M is extended from R if and only if $M_{\mathfrak{m}}$ is extended from $R_{\mathfrak{m}}$, for every $\mathfrak{m} \in \mathrm{Max}(R)$. □

Corollary 2.4.2. *Let R be a commutative ring and $A := R[x_1,\dots,x_n;\sigma]$. If for each $\mathfrak{m} \in \mathrm{Max}\,R$, $A_{\mathfrak{m}}$ is $\mathcal{E}$ with respect to $R_{\mathfrak{m}}$, then A is $\mathcal{E}$.*

Proof. Let $M \in \mathfrak{P}(A)$, then $M_{\mathfrak{m}} \in \mathfrak{P}(A_{\mathfrak{m}})$, and hence, by the hypothesis, $M_{\mathfrak{m}}$ is extended from $R_{\mathfrak{m}}$, for every $\mathfrak{m} \in \mathrm{Max}\,R$. Using Theorem 2.4.1 (note that M is finitely presented as A-module), M is extended from R, and hence, A is $\mathcal{E}$. □

2.5. Quillen-Suslin theorem

This last section concerns with Quillen-Suslin's theorem. Here R is non-commutative but some other extra conditions on it are assumed as well as over σ.

Theorem 2.5.1 (Horrocks' theorem)**.** *Let R be a left regular domain and Z its center. Suppose that Z is Noetherian, R is finitely generated over Z and σ is an automorphism of R of finite order d, with d invertible in Z. Suppose that $P \in \mathfrak{P}(A)$ is stably extended from R and the rank of P is at least 2. Then P is extended from R.*

Proof. Firstly we recall that the rank of P means the maximal number of R-independent elements of P, and P is stably extended from R is there exists $m \geq 0$ such that $P \oplus A^m$ is extended from R.
Denote by d the order of σ. The automorphism σ is mapping Z onto itself. Let Z^σ be the subalgebra in Z of invariants of σ. By Noether's theorem Z^σ is Noetherian and Z is a finitely generated Z^σ-module. We claim that $Z^\sigma[x_1^d,\dots,x_n^d]$ is a central subalgebra in A and A is

a finitely generated left $Z^\sigma[x_1^d, \dots, x_n^d]$-module. In fact monomials in $x_1, \dots, x_n$ commute. Since $x_i r = \sigma(r)x_i$ for any i and for any $r \in R$, then $x_i^d r = \sigma^d(r)x_i^d = rx^d$. Hence each element x_i^d is central. Now if $r \in Z^\sigma$ then r commutes with each element of R and with each variable x_i. Since R is a finitely generated Z-module then by Noether's theorem R is a finitely generated Z^σ-module. So the claim is proved.
Consider A as a graded ring $A = \oplus_n A_n$ where A_n is the span of all monomials of a total degree n. In particular $A_0 = R$ and $D = Z^\sigma[x_1^d, \dots, x_n^d]$ is a central homogeneous subalgebra such that A is a finitely generated D-modules.
For any nonzero homogeneous element $\alpha \in D_n = D \cap A_n$ following [9] denote by A_α^+ the graded ring consisting of a sum of non-negative summands from $\mathbb{Z}$-graded localized ring A_α. Similarly for any homogeneous ideal $\mathfrak{m}$ in D denote by $A_\mathfrak{m}^+$ the sum of non-negative graded summands from $\mathbb{Z}$-graded localized ring $A_\mathfrak{m}$ [9, Definition 5.30].

Lemma 2.5.2 ([9], Homogeneous analog of Patching Theorem from §4)**.** *Let V_n be the set consisitng of zero and nonzero elements $\alpha \in D_n$ such that P is extended from $A_\alpha^+(0)$. Then $V = \oplus_n V_n$ is a homogeneous ideal in D. Moreover if $\alpha^m \in V$ for some homogeneous element $\alpha \in D$, then $\alpha \in V$.*

If V contains $\sum_{i\geqslant m} V_i$ for some m then $m = 1$. Moreover by [9, Corollary 5.36] the ideal V contains $x_1^d, \dots, x_n^d$, and therefore the module P is extended from R since x_i^d is a monic polynomial in x_i.
Suppose that V is a proper ideal which does not contain $\sum_{i\geqslant m} V_i$ for any m. Then the ideal V is an intersection of prime homogeneous ideals. Hence we can replace A by a localized ideal $A_\wp^+$ for some homogeneous maximal ideal $\wp$ in D. As it was shown in [9, Corollaries 5.36] the ring $A_\wp^+$ is a skew polynomial extension $A_\wp^+(0)[x_i, \alpha]$ for some x_i. Using the restriction on the rank of P we can find a monic polynomial f in x_i such that P_f is extended from R. So by [9, Proposition 5.35] the module P is again extended from R. □

Theorem 2.5.3 (Quillen-Suslin)**.** *Let K be a field and $A := K[x_1, \dots, x_n; \sigma]$, with σ bijective and having finite order. Then A is $\mathcal{PF}$.*

Proof. Apply Theorem 2.5.1 with $R = Z = K$. □

2.6. Matrix-constructive proof of Quillen-Suslin theorem

In this section we present an elementary matrix-constructive proof of Theorem 2.5.3 for the case of only one variable; in this particular situation we can consider that K is a division ring and that we have a non trivial σ-derivation δ of K, where σ is bijective (but not necessarily of finite order). The main idea of the proof is to use the matrix characterization of $\mathcal{PF}$ rings given in Theorem 1.1.3. In Section 4.3 we will show an algorithm for this theorem.

Theorem 2.6.1 (Quillen-Suslin)**.** *Let K be a division ring and $A := K[x; \sigma, \delta]$, with σ bijective. Then A is $\mathcal{PF}$.*

Proof. Let $s \geq 1$ and let $F = [f_{ij}] \in M_s(A)$ be an idempotent matrix, the proof is by induction on s and we will follow a procedure as in Proposition 64 of [27]. We will use the relations that satisfy the entries of F, in particular, the following two relations:

$$f_{11}^2 + f_{12}f_{21} + f_{13}f_{31} + \cdots + f_{1s}f_{s1} = f_{11},$$
$$f_{11}f_{12} + f_{12}f_{22} + f_{13}f_{32} + \cdots + f_{1s}f_{s2} = f_{12}.$$

s=1: In this case $F = [f]$; since A is a domain, its idempotents are trivial, then $f = 1$ or $f = 0$ and hence $U = [1]$.
s $\geq$ 2: Now suppose that the result holds for $s - 1$ and let $F = [f_{ij}] \in M_s(A)$ be an idempotent matrix. We have two possibilities.
(A) All elements in the first row and in the first column of F are zero. Then we apply induction.
(B) Suppose that there exists at least one non zero element in the first row (the reasoning for the first column is similar); we can assume that $f_{11} \neq 0$ (if $f_{11} = 0$ and $f_{1j} \neq 0$ then we can change F by TFT^{-1} with $T := I_s - E_{j1}$). Then arise two possibilities.
(B1) $\deg(f_{11}) = 0$, so $f_{11} \in K - 0$, i.e., f_{11} is invertible. Then taking

$$U := \begin{bmatrix} 1 & f_{11}^{-1}f_{12} & f_{11}^{-1}f_{13} & \cdots & f_{11}^{-1}f_{1s} \\ -f_{21}f_{11}^{-1} & 1 & 0 & \cdots & 0 \\ -f_{31}f_{11}^{-1} & 0 & 1 & \cdots & 0 \\ \vdots & & & \cdots & \\ -f_{s1}f_{11}^{-1} & 0 & 0 & \cdots & 1 \end{bmatrix}$$

we have that $U \in GL_s(A)$ and its inverse is

$$U^{-1} = \begin{bmatrix} f_{11} & -f_{12} & -f_{13} & \cdots & -f_{1s} \\ f_{21} & -f_{21}f_{11}^{-1}f_{12} + 1 & -f_{21}f_{11}^{-1}f_{13} & \cdots & -f_{21}f_{11}^{-1}f_{1s} \\ f_{31} & -f_{31}f_{11}^{-1}f_{12} & -f_{31}f_{11}^{-1}f_{13} + 1 & \cdots & -f_{31}f_{11}^{-1}f_{1s} \\ \vdots & & & \cdots & \\ f_{s1} & -f_{s1}f_{11}^{-1}f_{12} & -f_{s1}f_{11}^{-1}f_{13} & \cdots & -f_{s1}f_{11}^{-1}f_{1s} + 1 \end{bmatrix}.$$

Moreover, $UFU^{-1} = \begin{bmatrix} 1 & 0_{1,s-1} \\ 0_{s-1,1} & F_1 \end{bmatrix}$, where $F_1 \in M_{s-1}(A)$ is an idempotent matrix, therefore we can apply induction.
(B2) $\deg(f_{11}) := n \geq 1$; since A is a domain at least one non diagonal entry in the first row and in the first column of F are non zero: In fact, if $f_{12} = \cdots = f_{1s} = 0$, then $f_{11} = 1$ or $f_{11} = 0$, false (similarly if $f_{21} = \cdots = f_{s1} = 0$). Using elementary and permutation matrices, no affecting the entry f_{11}, we can reduce the degrees of $f_{12}, \ldots, f_{1s}$ until the situation in which $f_{12} \neq 0$ and $f_{13} = \cdots = f_{1s} = 0$ (a similar reasoning apply for the first column); then we have $f_{11}^2 + f_{12}f_{21} = f_{11}$ and $f_{21} \neq 0$; note that $\deg(f_{11}^2) = 2n$, so $\deg(f_{21}) := p \leq n$ or $\deg(f_{12}) := q \leq n$; let $a_n := lc(f_{11})$, $c_p := lc(f_{21})$ and $b_q := lc(f_{12})$.

If $p \leq n$ then

$$TFT^{-1} = F' = \begin{bmatrix} f'_{11} & f'_{12} & f'_{13} & \cdots & f'_{1s} \\ f_{21} & f'_{22} & f_{23} & \cdots & f_{2s} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ f_{s1} & f'_{s2} & f_{s3} & \cdots & f_{ss} \end{bmatrix},$$

with

$$T := I_s - a_n\sigma^{n-p}(c_p^{-1})x^{n-p}E_{12};$$

note that F' is idempotent; moreover $f'_{11} = 0$ or $f'_{11} \neq 0$; if $f'_{11} \neq 0$ then arise two options: $\deg(f'_{11}) = 0$, i.e., $f'_{11} \in K - 0$ or $1 \leq \deg(f'_{11}) \leq n - 1$ and again $\deg(f_{21}) \leq \deg f'_{11}$ or $\deg(f'_{12}) \leq \deg f'_{11}$.
If $p > n$ but $q \leq n$ then

$$LFL^{-1} = F'' = \begin{bmatrix} f''_{11} & f_{12} & f_{13} & \cdots & f_{1s} \\ f''_{21} & f''_{22} & f''_{23} & \cdots & f''_{2s} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ f''_{s1} & f_{s2} & f_{s3} & \cdots & f_{ss} \end{bmatrix},$$

with

$$L := I_s + \sigma^{-q}(b_q^{-1}a_n)x^{n-q}E_{21};$$

note that F'' is idempotent; moreover $f''_{11} = 0$ or $f''_{11} \neq 0$; if $f''_{11} \neq 0$ then arise two options: $\deg(f''_{11}) = 0$, i.e., $f''_{11} \in K - 0$ or $1 \leq \deg(f''_{11}) \leq n - 1$ and again $\deg(f_{12}) \leq \deg f''_{11}$ or $\deg(f''_{21}) \leq \deg f''_{11}$.
We can repeat this reasoning for F' and F'' and we obtain an idempotent matrix $G = [g_{ij}]$ similar to F with $g_{11} = 0$ or $g_{11} \in K - 0$; if $g_{11} \in K - 0$ we conclude using the case (B1). Then assume that $g_{11} = 0$; if all elements in the first row and in the first column of G are zero, then we can apply induction and we finish. If not, then in a similar way as was remarked above, using elementary and permutation matrices, no affecting the first column, in particular the entry g_{11}, we can reduce the degrees of $g_{12}, \ldots, g_{1s}$ until the situation in which $g_{12} \neq 0$ and $g_{13} = \cdots = g_{1s} = 0$ (a similar reasoning apply for the first column); thus, from $g_{12}g_{22} = g_{12}$ we obtain that $g_{22} = 1$ and hence by the permutation matrix P_{12} we finish using the case (B1). □

2.7. Noether normalization lemma for Ore extensions

We conclude this chapter proving the Noether normalization lemma for Ore extensions with automorphism of finite order. This lemma is a key result for an eventual matrix-constructive proof of Theorem 2.5.3 for $n \geq 2$ variables (see Remark 2.7.2)
We recall the following notation: Let $F = [f_{ij}] \in M_s(A)$ be an idempotent matrix, where $A := K[x_1, \ldots, x_n; \sigma]$, K a field and σ an automorphism of K; for $w \in A$, $\deg(w)$ denotes the total degree of w (Definition 1.3.7); observe that $A = R[x_n; \sigma]$, with $R := K[x_1, \ldots, x_{n-1}; \sigma]$

and $\sigma : R \to R$ defined by $x_i \mapsto x_i$, $1 \leq i \leq n-1$, $\lambda \mapsto \sigma(\lambda)$, $\lambda \in K$. Besides, we will use the deglex order on $Mon(A)$ (see Definition 1.4.1)

Lemma 2.7.1 (Noether normalization). *Let $p := p(x_1, \ldots, x_n) \in A$, where σ has order finite t, and let*

$m := \min\{kt \mid kt > \deg(p), k \in \mathbb{Z}^+\} + 1.$

(i) The function defined by

$$x_n \mapsto x_n, \quad x_i \mapsto x_i - x_n^{m^{n-i}}, 1 \leq i \leq n-1$$

is an automorphism of A.

(ii) Let $y_n := x_n$ and $y_i := x_i - x_n^{m^{n-i}}, 1 \leq i \leq n-1$. Then $A = K[y_1, \ldots, y_n; \sigma]$ is an Ore extension of K in the variables $y_1, \ldots, y_n$. Moreover, $A \cong R[y_n; \sigma]$, with $R := K[y_1, \ldots, y_{n-1}; \sigma]$.

(iii) $p(y_1, \ldots, y_n) = \lambda p'(y_n)$, with $\lambda \in K - \{0\}$ and $p'(y_n) \in R[y_n; \sigma]$ monic.

Proof. (i) Note that $K[x_1, \ldots, x_n; \sigma] = K\{x_1, \ldots, x_n\}/I$, with

$$I := \langle x_j x_i - x_i x_j, x_i\lambda - \sigma(\lambda)x_i | 1 \leq i, j \leq n, \lambda \in K\rangle,$$

so we define the homomorphism of K-algebras

$$\alpha : K\{x_1, \ldots, x_n\} \to K\{x_1, \ldots, x_n\}/I, \;\; x_n \mapsto \overline{x_n}, \, x_i \mapsto \overline{x_i - x_n^{m^{n-i}}}, \, 1 \leq i \leq n-1;$$

note that $\alpha(I) = 0$. This induces an endomorphism

$$\overline{\alpha} : K[x_1, \ldots, x_n; \sigma] \to K[x_1, \ldots, x_n; \sigma], \, \overline{x_n} \mapsto \overline{x_n}, \, \overline{x_i} \mapsto \overline{x_i - x_n^{m^{n-i}}}.$$

It is clear that $\overline{\alpha}$ is bijective with inverse defined by

$$\overline{x_n} \mapsto \overline{x_n}, \, \overline{x_i} \mapsto \overline{x_i + x_n^{m^{n-i}}}, \, 1 \leq i \leq n-1.$$

Using the notation $x_i := \overline{x_i}$ we obtain (i).
(ii) Let k, $\ell \in \mathbb{Z}^+$ and $\lambda \in K$, then:

(a) $(kt+1)^\ell = \alpha_1 t + \alpha_2 t + \cdots + \alpha_\ell t + 1 = (\sum_{i=1}^{\ell} \alpha_i)t + 1$, for some $\alpha_1, \ldots, \alpha_\ell \in \mathbb{Z}^+$.

(b) $\sigma^{kt}(\lambda) = \lambda$.

(c) $\sigma^{(kt+1)^\ell}(\lambda) = \sigma^{\beta t}(\sigma(\lambda)) = \sigma(\lambda)$, with $\beta = \sum_{i=1}^{\ell} \alpha_i$., Thus, $\sigma^{m^\ell}(\lambda) = \sigma(\lambda)$.

(d) $y_n\lambda = x_n\lambda = \sigma(\lambda)x_n = \sigma(\lambda)y_n$, and for $1 \leq i \leq n-1$,

$$y_i\lambda = (x_i - x_n^{m^{n-i}})\lambda = \sigma(\lambda)x_i - \sigma^{m^{n-i}}(\lambda)x_n^{m^{n-i}} = \sigma(\lambda)x_i - \sigma(\lambda)x_n^{m^{n-i}} = \sigma(\lambda)y_i.$$

(e) $y_i y_j = y_j y_i$ for every $1 \leq i, j \leq n$.

From these remarks and (i), we get that $A = K[y_1, \ldots, y_n; \sigma]$ is an Ore extension of K in the variables $y_1, \ldots, y_n$ where the monomials $y_1^{j_1} \cdots y_n^{j_n}$, $j_i \geq 0$, $1 \leq i \leq n$, conform a K-basis of A.
In order to prove the second statement of (ii) note that $R := K[y_1, \ldots, y_{n-1}; \sigma]$ is an Ore extension of K in the variables $y_1, \ldots, y_{n-1}$; moreover,

$$\sigma : R \to R,\ y_i \mapsto y_i,\ 1 \leq i \leq n-1,\ \lambda \mapsto \sigma(\lambda),\ \lambda \in K$$

is an endomorphism of R. Considering the universal property of R viewed as a skew PBW extension of K (see [1]), and in turn, the universal property of $R[y_n; \sigma]$, we get that $A \cong R[y_n; \sigma]$.
(iii) The proof of this part is an easy adaptation of the classical commutative case. We denote the n-tuple $(m^{n-1}, m^{n-2}, \ldots, m, 1)$ by (m), and by (j) a n-tuple $(j_1, \ldots, j_n)$, with $j_i \geq 0$. El dot product $(m) \cdot (j)$ is defined by

$$(m) \cdot (j) := m^{n-1} j_1 + \cdots + m j_{n-1} + j_n.$$

The polynomial p can be written as a finite sum $p = \sum_{(j)} \lambda_{(j)} x_1^{j_1} \ldots x_n^{j_n}$, where $\lambda_{(j)} \in K - \{0\}$. Replacing each x_i we get $p = \sum_{(j)} \lambda_{(j)} (y_1 + y_n^{m^{n-1}})^{j_1} \ldots (y_{n-1} + y_n^m)^{j_{n-1}} y_n^{j_n}$. Expanding each binomial we obtain

$$p = \sum_{(j)} \lambda_{(j)} y_n^{(m)\cdot(j)} + \sum_{(j)} f_{(j)}(y_1, \ldots, y_{n-1}, y_n),$$

where each polynomial $f_{(j)}(y_1, \ldots, y_{n-1}, y_n)$ includes some y_i to a positive power and the highest power of y_n in these polynomials is strictly less than $(m) \cdot (j)$. By induction on n we can prove that if $(j) \neq (j')$ then $(m) \cdot (j) \neq (m) \cdot (j')$. Thus, all the exponents $(m) \cdot (j)$ are different, and hence, all the terms $\lambda_{(j)} y_n^{(m)\cdot(j)}$ are distinct. If d is the largest $(m).(j)$, then d is the degree of p as a polynomial in y_n with coefficients in $R = K[y_1, \ldots, y_{n-1}; \sigma]$. Hence,

$$p = \lambda y_n^d + g(y_1, \ldots, y_{n-1}, y_n),$$

where $\lambda \in K - 0$ and g has degree in y_n strictly less than d. Since $\lambda \neq 0$ and K is a filed, we set

$$p' = y_n^d + \lambda^{-1} g(y_1, \ldots, y_{n-1}, y_n),$$

i.e., $p(y_1, \ldots, y_n) = \lambda p'(y_n)$, with $\lambda \in K - \{0\}$ and $p'(y_n) \in R[y_n; \sigma]$ monic. □

Remark 2.7.2. Theorem 2.6.1 gives a constructive proof of Theorem 2.5.3 for one single variable; we would like to present a matrix-constructive proof of this fact for $n \geq 2$ variables. Assuming the next not proved yet lemma, and using the Noether normalization lemma, we can show the claimed.
Lemma. Let $F = [f_{ij}] \in M_s(A)$ be an idempotent matrix with $f_{11} \in R[x_n; \sigma]$ monic with σ of finite order, where $R := K[x_1, \ldots, x_{n-1}; \sigma]$. Then F is similar to an idempotent matrix $F' \in M_s(R)$.
Theorem. Quillen-Suslin for $n \geq 2$ variables. Let K be a field and $A := K[x_1, \ldots, x_n; \sigma]$, with σ bijective of finite order. Then A is $\mathcal{PF}$.

Proof. The proof is by induction on n. For $n = 1$ the result follows from Theorem 2.6.1 taking $\delta = 0$. So, assume that $n \geq 2$. Let $s \geq 1$ and $F = [f_{ij}] \in M_s(A)$ be idempotent. The idea is to apply Theorem 1.1.3. We proceed by induction on s.

s=1: In this case $F = [f]$ with $f \in A$; since A is a domain, its idempotents are $f = 1$ or $f = 0$, whence F is trivially similar to a matrix as in Theorem 1.1.3.

s $\geq$ **2**: Suppose that the result holds for $s - 1$. We have two possibilities.

(A) All elements in the first row and in the first column of F are zero. Then we apply the induction on s.

(B) Suppose that there exists at least one non zero element in the first row (the reasoning for the first column is similar); we can assume that $f_{11} \neq 0$ (if $f_{11} = 0$ and $f_{1j} \neq 0$, then we can change F by TFT^{-1} with $T := I_s - E_{j1}$). By Lemma 2.7.1 we can suppose that $f_{11} \in R[x_n; \sigma]$ is monic, where $R := K[x_1, \ldots, x_{n-1}; \sigma]$. Then the theorem follows from the above Lemma and applying induction on n. □

3. Applications

The convolutional codes have been intensively studied (see [21], [23], [30], [31], [32], [33], [60], [61], [62], [69], [70], [77]) and they are supported by algebraic structures related to direct summands of free modules over classical polynomial rings. Piret in [62] proposed to study the problem over skew polynomial rings. In [33] it is used the notion of a separable ring extension in ideal codes with structure over a $A[x;\sigma,\delta]$, when A is a semisimple algebra; there in the authors show that ideal codes are generated by idempotent elements, and using a suitable separability element, they design an efficient algorithm for computing these idempotents. In this chapter we introduce a natural adaptation of the multidimensional ideal code for the the multivariable Ore extension $A[x_1,\ldots,x_n;\sigma]$, with A semisimple algebra and assuming some suitable conditions of separability.

3.1. Multidimensional Convolutional codes

3.1.1. Separability and Ore extensions

Let A, B, C be rings, M ne an (A,B)-bimodule, and N be an (B,C)-bimodule. Then its tensor product $M\otimes_B N$ becomes in an (A,C)-bimodule in the usual way. For a homomorphism of rings $\alpha : B \longrightarrow A$, we consider the canonical B-bimodule structure for A with actions $ba = \alpha(b)a$, $ab = a\alpha(b)$, for all $a \in A$ and $b \in B$. Thus, A becomes both an (A,B)-bimodule and an (B,A)-bimodule.
The following classical notion of a separable algebra over a commutative ring is a key conceptual tool in this chapter (see, [33],[37]).

Definition 3.1.1. *([37], Definition 2). A homomorphism of rings $\alpha : B \longrightarrow A$ is said to be a separable ring extension if the multiplication map $\mu : A\otimes_B A \longrightarrow A$, that maps $a\otimes a'$ onto aa', is a split epimorphism of A-bimodules. Equivalently, there exists an element $p=\sum_i a_i\otimes b_i \in A\otimes_B A$ (called a separability element) such that $ap = pa$ for all $a\in A$ and $\mu(p) = 1$, that is, for all $a \in A$,*

$$\sum_i aa_i\otimes b_i = \sum_i a_i\otimes b_i a, \tag{3-1}$$

and

$$\mu\Big(\sum_i a_i\otimes b_i\Big) = \sum_i a_i b_i = 1. \tag{3-2}$$

Remark 3.1.2. If $\alpha : B \longrightarrow A$ is a separable ring extension, then α is injective. In fact, if $\alpha(b) = 0$ for $b\in B$, then $b = b\mu(p) = \mu(bp) = \mu(\alpha(b)p) = \mu(0) = 0$. Thus, a separable ring extension is often denoted by $B \subseteq A$, even though that α needs not to be an inclusion of sets.

The following result is an important tool (see, [33] corollary 3).

Proposition 3.1.3. *Let $B \subseteq A$ be a separable ring extension with separability element $p = \sum_i ai \otimes b_i \in A \otimes_B A$. Consider a left ideal I of A which is a B-direct summand of A with B-split exact sequence, where $\iota : A/I \to A$ is such that $\pi\iota = id_{A/I}$:*

$$0 \longrightarrow I \longrightarrow A \xrightarrow{\pi} A/I \longrightarrow 0.$$

Then I is an A-direct summand of A with A-split exact sequence

$$0 \longrightarrow I \longrightarrow A \xrightarrow{\pi} A/I \longrightarrow 0,$$

where $\beta : A/I \to A$ is such that $\pi\beta = id_{A/I}$ and

$$\beta(r + I) = \sum_i a_i \iota(b_i r + I)$$

for every $a + I \in A/I$. Thus, $I = Re$, where $e \in A$ is the idempotent and $e = 1 - f$, with

$$f = \beta(1 + I) = \sum_i a_i \iota(b_i + I).$$

3.1.2. Separable Ore extensions

Let σ be an endomorphism of a ring A. A (left) σ-derivation is an additive map $\delta : A \longrightarrow A$ such that $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for all $a, b \in A$. Given σ, the set of all σ-derivations is denoted by $Der^\sigma(A)$. Let B be a subring of A such that $\sigma(B) \subseteq B$ and $\delta(B) \subseteq B$ for some $\delta \in Der^\sigma(A)$. Even though that σ and δ need not to be B-bimodule maps, it is possible to extend them to maps $\sigma^\otimes, \delta^\otimes : A \otimes_B A \longrightarrow A \otimes_B A$ as the following lemma shows.

Lemma 3.1.4. *Let $B \subseteq A$ be a ring extension, σ an endomorphism of A, and $Der^\sigma(A)$. If $\sigma(B) \subseteq B$ and $\delta(B) \subseteq B$, then the maps*

$$\begin{aligned} \sigma^\otimes : A \otimes_B A &\longrightarrow A \otimes_B A \\ a \otimes b &\longmapsto \sigma(a) \otimes \sigma(b) \\ \delta^\otimes : A \otimes_B A &\longrightarrow A \otimes_B A \\ a \otimes b &\longmapsto \sigma(a) \otimes \delta(b) + \delta(a) \otimes b \end{aligned}$$

are well defined.

Proof. It is enough to check that $\sigma^\otimes(as \otimes b) = \sigma^\otimes(a \otimes sb)$ for each $s \in B$ and all $a, b \in A$.

$$\begin{aligned} \sigma^\otimes(as \otimes b) &= \sigma(as) \otimes \sigma(b) \\ &= \sigma(a)\sigma(s) \otimes \sigma(b) \\ &= \sigma(a) \otimes \sigma(s)\sigma(b) \\ &= \sigma(a) \otimes \sigma(sb) \\ &= \sigma^\otimes(a \otimes sb), \end{aligned}$$

analogously,

$$\begin{aligned}\delta^{\otimes}(as\otimes b)&=\sigma(as)\otimes\delta(b)+\delta(as)\otimes b\\&=\sigma(a)\sigma(s)\otimes\delta(b)+(\sigma(a)\delta(s)+\delta(a)s)\otimes b\\&=\sigma(a)\otimes\sigma(s)\delta(b)+\sigma(a)\otimes\delta(s)b+\delta(a)\otimes sb\\&=\sigma(a)\otimes(\sigma(s)\delta(b)+\delta(s)b)+\delta(a)\otimes sb\\&=\sigma(a)\otimes\delta(sb)+\delta(a)\otimes sb\\&=\delta^{\otimes}(a\otimes sb).\end{aligned}$$

Thus $\sigma^{\otimes}$ and $\delta^{\otimes}$ are well defined. □

Remark 3.1.5. Note that if $p \in A \otimes_B A$ is a separability element of $B \subseteq A$, and σ is an automorphism of A such that $\sigma(B) \subseteq B$, then $\sigma^{\otimes}(p)$ is a separability element of $B \subseteq A$: In fact, let $r = \sigma^{-1}(r') \in A$ and $p = \sum_i a_1 \otimes b_i$, then

$$r\sigma^{\otimes}(p)=\sum_i \sigma(r'a_i)\otimes\sigma(b_i)=\sigma^{\otimes}\Big(\sum r'a_i\otimes b_i\Big)=\sigma^{\otimes}\Big(\sum a_i\otimes b_i r'\Big)=\sigma^{\otimes}(p)r,$$

and

$$\mu(\sigma^{\otimes}(p))=\mu\Big(\sum_i \sigma(a_i)\otimes\sigma(b_i)\Big)=\sum_i \sigma(a_i)\sigma(b_i)=\sum_i \sigma(a_ib_i)=\sigma\Big(\sum_i a_ib_i\Big)=1.$$

Recall that the Ore extension $A[x_1,\dots,x_n;\sigma]$ of A, where σ is a ring endomorphism of A, is a skew PBW extensions where the free left A-basis are the monomials x^{α}, and the multiplication is defined by the rules

$$x_ia=\sigma(a)x_i,\ \text{for all } a\in A \text{ and } x_ix_j=x_jx_i \text{ for all } 1\le i,j\le n.$$

In order to prove the main result of this section we need to introduce some notation. Let $B \subseteq A$ such that $\sigma(B) \subseteq B$, and let $R := A[x_1,\dots,x_n;\sigma]$ and $S := B[x_1,\dots,x_n;\sigma_{|B}]$. Let ϕ be the morphism of A-bimodules defined as the composition of the canonical morphisms

$$\phi : A\otimes_B A \longrightarrow R\otimes_B R\longrightarrow R\otimes_S R.$$

Theorem 3.1.6. *Let $B \subseteq A$ be a separable ring extension with separability element $p \in A \otimes_B A$. Let σ be an endomorphism of A such that $\sigma(B) \subseteq B$. If $\sigma^{\otimes}(p) = p$ then*

$$B[x_1,\dots,x_n;\sigma_{|B}]\subseteq A[x_1,\dots,x_n;\sigma]$$

is a separable ring extension with separability element $\overline{p} := \phi(p)$.

Proof. Let R, S, ϕ and p as before. Then $\overline{p} = \phi(p) = \sum_i a_i \otimes_S b_i$.
For each $a \in A$,

$$a\overline{p}=a\phi(p)=\phi(ap)=\phi(pa)=\phi(p)a=\overline{p}a,$$

now for x_j, with $1 \leq j \leq n$, we have:

$$\begin{aligned}
x_j\overline{p} &= \sum_i x_j a_i \otimes_S b_i \\
&= \sum_i \sigma(a_i) x_j \otimes_S b_i \\
&= \sum_i \sigma(a_i) \otimes_S x_j b_i \\
&= \sum_i \sigma(a_i) \otimes_S \sigma(b_i) x_j \\
&= \left(\sum_i \sigma(a_i) \otimes_S \sigma(b_i) \right) x_j \\
&= \phi \left(\sum_i \sigma(a_i) \otimes_B \sigma(b_i) \right) x_j \\
&= \phi(\sigma^{\otimes}(p)) x_j \\
&= \phi(p) x_j = \overline{p} x_j.
\end{aligned}$$

Besides, $\mu(\overline{p}) = \sum_i a_i b_i = 1$, and the proof is over. □

Now we get a fundamental type of separable Ore extensions.

Definition 3.1.7. *Let $\mathbb{F} = \mathbb{F}_q \subseteq \mathbb{F}_{q^t}$ be a finite field extension. Let $\sigma = \tau^h$ be an $\mathbb{F}$-automorphism, where τ denotes the Frobenius automorphism of the extension.*

Proposition 3.1.8. *Let $\mathbb{F}$, $\mathbb{F}_{q^t}$ and $\sigma = \tau^h$ as in Definition 3.1.7. Then the ring extension*

$$\mathbb{F}[x_1, \ldots, x_n] \subseteq \mathbb{F}_{q^t}[x_1, \ldots, x_n; \sigma]$$

is separable.

Proof. We will exhibit a separability element $p \in \mathbb{F}_{q^t} \otimes_F \mathbb{F}_{q^t}$ of the extension $F \subseteq \mathbb{F}_{q^t}$ such that $\sigma^{\otimes}(p) = p$. Following [55] for basic facts concerning finite fields, in particular, we follow the notation and properties about the trace function. It is well known that a separability element can be obtained from dual basis. The dual basis of a normal basis is also normal, hence let $\{a, a^q, \ldots, a^{q^{t-1}}\}$, $\{b, b^q, \ldots, b^{q^{t-1}}\}$ be normal dual bases. We are going to check that $p = \sum_i a^{q^i} \otimes b^{q^i} \in \mathbb{F}_{q^t} \otimes_{\mathbb{F}} \mathbb{F}_{q^t}$ is a separability element. Dual basis are characterized by the equalities

$$z = \sum_i Tr_{\mathbb{F}_{q^t}/\mathbb{F}}(b^{q^i} z) a^{q^i} = \sum_i Tr_{\mathbb{F}_{q^t}/\mathbb{F}}(a^{q^i} z) b^{q^i}$$

for all $z \in \mathbb{F}_{q^t}$. Hence

$$\begin{aligned} zp &= \sum_i za^{q^i} \otimes b^{q^i} \\ &= \sum_i \Big(\sum_j Tr_{\mathbb{F}_{q^t}/\mathbb{F}}(b^{q^j} z a^{q^i}) a^{q^j} \Big) \otimes b^{q^i} \\ &= \sum_j \sum_i \big(Tr_{\mathbb{F}_{q^t}/\mathbb{F}}(a^{q^i} b^{q^j} z) a^{q^j} \otimes b^{q^i} \big) \\ &= \sum_j a^{q^j} \otimes \sum_i Tr_{\mathbb{F}_{q^t}/\mathbb{F}}(a^{q^i} b^{q^j} z) b^{q^i} \\ &= \sum_i za^{q^i} \otimes b^{q^i} \\ &= pz, \end{aligned}$$

besides, $\sum_i a^{q^i} b^{q^i} = \sum_i (ab)^{q^i} = Tr_{\mathbb{F}_{q^t}/\mathbb{F}}(ab) = 1$ by duality. Since, $\sigma(w) = w^{q^h}$ for each $w \in \mathbb{F}_{q^t}$, we obtain that $\sigma(a^{q^i}) = a^{q^{i+h \ (mod t)}}$, similarly for b^{q^i}. Hence, we get that σ induce a permutation over $\{a, a^q, \ldots, a^{q^{t-1}}\}$ and $\{b, b^q, \ldots, b^{q^{t-1}}\}$, thus $\sigma^{\otimes}(p) = p$. So, p es separability element and as a consequence of Theorem 3.1.6 we have the result. □

3.2. Multidimensional codes generated by idempotents

Let $\mathbb{F} := \mathbb{F}_q$ be a finite field and let A a finite semisimple $\mathbb{F}$-algebra. Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$. Then $\mathbb{F}[x_1, \ldots, x_n]$ is a subring of the Ore extension $R := A[x_1, \ldots, x_n; \sigma]$. So, R can be considered as a $\mathbb{F}[x_1, \ldots, x_n]$-module. Let $V := \{v_0, \ldots, v_{m-1}\}$ a basis of A as $\mathbb{F}$-vector space, besides also a basis of R as $\mathbb{F}[x_1, \ldots, x_n]$-module, this is justified be the map

$$\begin{aligned} \alpha : \mathbb{F}[x_1, \ldots, x_n]^m &\longrightarrow R \\ \big(f_j(X)\big)_{j=0}^{m-1} &\longmapsto \sum_{j=0}^{m-1} v_j f_j(X) \end{aligned}$$

that is a $\mathbb{F}[x_1, \ldots, x_n]$-module isomorphism; letting

$$\alpha\big(\sum_i a_{ij} X^{\beta_i}\big)_{j=0}^{m-1} = \sum_{j=0}^{m-1} v_j \big(\sum_i a_{ij} X^{\beta_i}\big) = \sum_i \big(\sum_{j=0}^{m-1} a_{ij} v_j\big) X^{\beta_i}.$$

Next we define a multidimensional ideal code, i.e., a multidimensional convolutional code.

Definition 3.2.1. *A multidimensional ideal code is a $\mathbb{F}[x_1, \ldots, x_n]$-submodule direct summand C of $\mathbb{F}[x_1, \ldots, x_n]^n$ such that $\alpha(C)$ is a left ideal of R.*

Therefore, we can understand that a multidimensional ideal code is just a left ideal I of $R = A[x_1, \ldots, x_n; \sigma]$ which is a $\mathbb{F}[x_1, \ldots, x_n]$-direct summand of R. As a direct consequence of Proposition 3.1.3, we get.

Proposition 3.2.2. *If $\mathbb{F}[x_1, \ldots, x_n] \subseteq A[x_1, \ldots, x_n; \sigma]$ is a separable ring extension, then every multidimensional ideal code is a direct summand of $A[x_1, \ldots, x_n; \sigma]$ as a left ideal, and hence, it is generated by an idempotent of $A[x_1, \ldots, x_n; \sigma]$.*

Next we will show some consequences of the Proposition 3.2.2. From ([21]) we adapt the following definition.

Definition 3.2.3. *Let $\mathbb{F}[G]$ be the group algebra of a finite group G. Let $\sigma \in \mathrm{Aut}(\mathbb{F}[G])$. A multidimensional group convolutional code is a multidimensional ideal code in $\mathbb{F}[G][x_1, \ldots, x_n; \sigma]$.*

Proposition 3.2.4. *Let G be a finite group such that $(|G|, char\ \mathbb{F}) = 1$, let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{F}[G])$ such that $\sigma(G) = G$. Then each multidimensional group convolutional code is a direct summand of $R = \mathbb{F}[G][x_1, \ldots, x_n; \sigma]$ as a left ideal over R, and, hence generated by an idempotent of R.*

Proof. From Proposition 3.2.2, we need to prove that the ring extension $\mathbb{F}[x_1, \ldots, x_n] \subseteq A[x_1, \ldots, x_n; \sigma]$ is separable with $A = \mathbb{F}[G]$. It is easily checked that $p := |G|^{-1} \sum_{g \in G} g \otimes g^{-1} \in \mathbb{F}[G] \otimes_{\mathbb{F}} \mathbb{F}[G]$ is a separability element for the extension $\mathbb{F} \subseteq \mathbb{F}[G]$ such that $\sigma^{\otimes}(p) = p$. By Theorem 3.1.6, the extension $\mathbb{F}[x_1, \ldots, x_n] \subseteq R$ is separable, with separability element

$$\overline{p} = |G|^{-1} \sum_{g \in G} g \otimes_{\mathbb{F}[x_1, \ldots, x_n; \sigma]} g^{-1}, \tag{3-3}$$

therefore the proof is over. □

Proposition 3.2.5. *Let A be any finite semisimple commutative $\mathbb{F}$-algebra A, and σ an $\mathbb{F}$-automorphism of A. Then every multidimensional ideal code of $R = A[x_1, \ldots, x_n; \sigma]$ is a direct summand left ideal of R and, consequently, it is generated by an idempotent element of R.*

Proof. By Proposition 3.2.2, we need to show that $S := \mathbb{F}[x_1, \ldots, x_n] \subseteq R$ is separable. Let $\{e_1, \ldots, e_\ell\}$ be idempotents such that $A = \bigoplus_{i=1}^{\ell} Ae_i$ is a decomposition of A into simple blocks. Since A is commutative, Ae_i is a finite field extension of $\mathbb{F}$ for all $i = 1, \ldots, \ell$. We follow the notation of ([33], Theorem 14). Thus, for each $j = 1, \ldots, t$ (here t is as in [33], page 9), we have an $\mathbb{F}$-automorphism $\sigma_{j_{m_j}} \circ \cdots \circ \sigma_{j_1}$ (j_l as in [33], Theorem 14) of the finite field Ae_{j_1}. By Proposition 3.1.8, there is a separability element $p_j \in Ae_{j_1} \otimes Ae_{j_1}$ such that $(\sigma_{j_{m_j}} \circ \cdots \circ \sigma_{j_1})^{\otimes}(p_j) = p_j$. ([33], Theorem 14) gives then a separability element $p \in A \otimes A$ such that $\sigma^{\otimes}(p) = p$, and by the Theorem 3.1.6 we get that $S \subseteq R$ is a separable ring extension, with separability element

$$\overline{p} = \sum_{j=1}^{t} \sum_{k} \alpha_{jk} \otimes_S \beta_{jk} + \sum_{j=1}^{t} \sum_{i=1}^{m_j - 1} \sum_{k} \sigma_{j_i} \circ \cdots \circ \sigma_{j_1}(\alpha_{jk}) \otimes_S \sigma_{j_i} \circ \cdots \circ \sigma_{j_1}(\beta_{jk}), \tag{3-4}$$

where $\{\alpha_{jk}\}$ and $\{\beta_{jk}\}$ are dual basis of Ae_{j_1} over $\mathbb{F}$ for each $j = 1, \ldots, t$. □

Proposition 3.2.6. *Let ς be an automorphism of the matrix algebra $B = \mathcal{M}_t(\mathbb{F})$ of finite order m. Let $A := \bigoplus_{i=1}^{m} B_j$ with $B_j = B$ for each $j = 1, \dots, m$ and $\sigma : A \longrightarrow A$ be defined by*

$$\sigma(\beta_1, \dots, \beta_m) = (\varsigma(\beta_m), \varsigma(\beta_1), \dots, \varsigma(\beta_{m-1})),$$

for each $(\beta_1, \dots, \beta_m) \in A$. Then every multidimensional ideal code in $A[x_1, \dots, x_n; \sigma]$ is a left ideal direct summand and, therefore, it is generated by an idempotent of $A[x_1, \dots, x_n; \sigma]$.

Proof. By Proposition 3.2.2 we need to show that $S := \mathbb{F}[x_1, \dots, x_n] \subseteq A[x_1, \dots, x_n; \sigma]$ is a separable ring extension. Let e_k be the central idempotent of A with zeroes in all its components except the k-th, whose entry is 1. The elements of B_k can therefore be represented as be_k where $b \in B = \mathcal{M}_t(\mathbb{F})$. Let $p_1 \in B_1 \otimes B_1 = \mathcal{M}_t(\mathbb{F})e_1 \otimes \mathcal{M}_t(\mathbb{F})e_1$ be any separability element of the matrix algebra, thus,

$$p_1 = \sum_{i=1}^{t} E_{ij}e_1 \otimes E_{ji}e_1,$$

for some $j \in \{1, \dots, t\}$. Following the notation of ([33], Proposition 13), we have that $\sigma_i(be_i) = \varsigma(b)e_{i+1}$, thus $(\sigma_m \circ \cdots \circ \sigma_1)^{\otimes}(p_1) = (\varsigma^m)^{\otimes}(p_1) = p_1$. From ([33], Proposition 13),

$$p = p_1 + \sum_{i=1}^{m-1} (\sigma_i^{\otimes} \circ \cdots \circ \sigma_1^{\otimes})(p_1) \tag{3-5}$$

is a separability element of $\mathbb{F} \subseteq A$ such that $\sigma^{\otimes}(p) = p$. From Theorem 3.1.6 we finish the proof. □

3.3. Computation of the idempotent generator

In this section A is a finite dimensional semisimple algebra over a finite field $\mathbb{F}$ and let $\{v_0, \dots, v_{m-1}\}$ be a fixed basis of A as an $\mathbb{F}$-vector space. Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ and consider $R := A[x_1, \dots, x_n; \sigma]$. Assume that $S := F[x_1, \dots, x_n] \subseteq A[x_1, \dots, x_n; \sigma]$ is a separable ring extension and that a separability element $\overline{p} = \sum_i a_i \otimes_S b_i \in R \otimes_S R$ is given. Theorem 3.1.6 provides a way to obtain such an element from a suitable separability element for the extension $\mathbb{F} \subseteq A$. From Proposition 3.2.2 we have that every multidimensional ideal code given by a left ideal I of R must be a direct summand of R and, therefore, it is generated, as a left ideal of R, by an idempotent. The idea now is to describe an algorithm that computes this idempotent from a set of generators $L = \{g_0, \dots, g_{t-1}\}$ of I as a left ideal of R, whenever the separability element p of the extension $S \subseteq A[x_1, \dots, x_n; \sigma]$ is available. The explicit formula of a separability element is given for multidimensional group codes (3-3), multidimensional ideal codes over any commutative finite semisimple algebra (3-4), and for multidimensional ideal codes over some non-commutative finite semisimple algebras (3-5).
Let I be a left ideal of R. We have an exact sequence of left R-modules

$$R^t \xrightarrow{\ G\ } R \xrightarrow{\ \pi\ } R/I \longrightarrow 0.$$

where G is the homomorphism of left R-modules. We know that $\{v_0, \dots, v_{m-1}\}$ becomes a basis of the $\mathbb{F}[x_1, \dots, x_n]$-module R, and we have the isomorphism of $\mathbb{F}[x_1, \dots, x_n]$-modules.

$$\begin{aligned} \alpha : \mathbb{F}[x_1, \dots, x_n]^m &\longrightarrow R \\ \big(f_j(X)\big)_{j=0}^{m-1} &\longmapsto \sum_{j=0}^{m-1} v_j f_j(X) \end{aligned}$$

with inverse

$$\begin{aligned} \gamma : R &\longrightarrow \mathbb{F}[x_1, \dots, x_n]^m \\ \sum_i f_i X^{\beta_i} &\longmapsto \big(\sum_i f_{i,0} X^{\beta_i}, \dots, \sum_i f_{i,m-1} X^{\beta_i}\big) \end{aligned}$$

where, for each i, $f_i = v_0 f_{i,0} + \cdots + v_{m-1} f_{i,m-1}$. Then I is generated as a $\mathbb{F}[x_1, \dots, x_n]$-module by $\{g_j v_i \mid 0 \leq i \leq m-1, 0 \leq j \leq t-1\}$. Hence a generator matrix for I is

$$\begin{bmatrix} \gamma(g_0 v_0) & \cdots & \gamma(g_0 v_{m-1}) & \cdots & \cdots & \gamma(g_{t-1} v_0) & \cdots & \gamma(g_{t-1} v_{m-1}) \end{bmatrix} \tag{3-6}$$

and we get the exact sequences of $\mathbb{F}[x_1, \dots, x_n]$-modules

$$\begin{aligned} &R^t \xrightarrow{\ G\ } R \xrightarrow{\ \pi\ } R/I \longrightarrow 0, \\ &S^{tm} \xrightarrow{M(G)} S^m \xrightarrow{\ \pi\alpha\ } R/I \longrightarrow 0. \end{aligned}$$

The left ideal I is an multidimensional ideal code if and only if it is a S-direct summand of R, equivalently, if and only there exists invertible matrices P and Q such that

$$H := \begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix} = P \cdot M(G) \cdot Q.$$

If the matrix H has this form it is called *basic*.

4. Implementation of skew PBW extensions with Maple

This chapter is dedicated to implement in Maple the theory of Gröbner basis of skew PBW extensions, as well as, some of its important applications in homological algebra. The main algorithms of any theory of Gröbner basis are the Division Algorithm and the Buchberger's Algorithm that computes the Gröbner bases. We have implemented these algorithms not only for left ideals, but also for submodules of A^m, where A is a skew PBW extension. As was pointed out in Remark 1.4.5, our hypothesis for this implementation are the following: We will assume that $A = \sigma(R)\langle x_1, \dots, x_n\rangle$ is a bijective skew PBW extension of a $\mathcal{LGS}$ ring R and $Mon(A)$ is endowed with some monomial order $\succeq$.
We have chosen three homological applications: (a) The computation of syzygies of left ideals, or more general, the computation of syzygies of submodules of A^m; (b) the computation of free resolutions of a given submodule of A^m; (c) the left inverse of a rectangular matrix over A.
We have added a special section in which we have computed the matrix U and the basis involved in the constructive proof of Quillen-Suslin theorem for Ore extensions (Theorem 1.1.3).

4.1. Gröbner theory of skew PBW extensions with Maple

In this section we present a library developed in Maple® 2016 that allows to use the skew PBW extensions computationally, and also, to calculate the Gröbner bases over them. This implementation let us to make effective some homological applications of skew PBW extensions (see [24], [27], [45], [51] and [52]). In this section each performed example uses the mentioned library.
We developed a library called `SPBWE.lib` consisting of the packages: `RingTools`, `SPBWETools`, `SPBWEGrobner` and `SPBWERings` (see, Appendices A and B).

- `RingTools`: This allows to define the structure of the ring R of coefficients of a skew PBW extension A.
- `SPBWETools`: This is a collection of functions related to the skew PBW extensions, these tools allow to define the structure of a skew PBW extension and they are very useful for working with these noncommutative rings of polynomial type.
- `SPBWEGrobner`: This is a collection of functions related to the Gröbner bases over skew PBW extensions, the main routine is the version of the Buchberger's Algorithm for bijective skew PBW extensions.

- `SPBWERings`: This is a collection of predefined subclasses of the skew PBW extensions.

4.1.1. Defining skew PBW extensions

In this section we present some examples that illustrate how to define skew PBW extensions using the packages mentioned before. Some easy computations are included. For more details see Appendix A.
From ([1] Definition 2.1) we can define a skew PBW extension $A := \sigma(R)\langle x_1 \dots, x_n\rangle$ using the following parameters:

`SetSkewPBWExtension(`L_1`,`L_1`,`L_3`,`L_4`,`C`)`

$L_1 :=$ List of variables $x_1, \dots, x_n$, assuming $x_1 \succ \cdots \succ x_n$.
$L_2 :=$ List of relations among variables x_i for $1 \leq i \leq n$.
$L_3 :=$ List of automorphisms σ_i for $1 \leq i \leq n$.
$L_4 :=$ List of σ-derivations, δ_i for $1 \leq i \leq n$.
$C :=$ The ring R of coefficients.

Remark 4.1.1. The parameter C can be omitted if the ring of coefficients is some subring of $\mathbb{C}(t_1, \dots, t_m)$, where $t_i \notin \{x_1, \dots, x_n\}$, $1 \leq i \leq m$, more exactly, a default ring C can be someone of the following rings:

$$S, \qquad S[t_1, \dots, t_m], \qquad S(t_1, \dots, t_m), \text{ where } S \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}. \tag{4-1}$$

Example 4.1.2. Univariate skew polynomial ring.
Let $A := \mathbb{Z}_{12}[t][x; \sigma, \delta]$, where $\sigma(p(t)) := p(t-1)$ and $\delta(t) = 1$. Here we have

$$\delta\Big(\sum_i a_i t^i\Big) = \sum_i a_i \delta(t^i) \quad \text{and} \quad \delta(t^n) = \sum_{k=0}^{n-1} \sum_{i=0}^{n-k-1} \binom{n-k-1}{i} (-1)^i t^{n-i-1}.$$

Define the coefficients ring using:
R`:=SetCoeffsRing(Name=`$K[t]$`,chr=12):` %% R is defined as $K[t]$.
%% t is not declared.
%% K is a ring with $\mathrm{char}(K) = 12$.
The implementation of A is given by

$A :=$ `SetSkewPBWExtension([`x`],[],[`σ`],[`δ`],R).`

We get $A = \sigma(R)\langle x\rangle$. Let us to show a simple calculation in A: Let $z_1 := x^2 + tx + 4x + t$ and $z_2 := t + 4 + 3x$, then

$$z_1 \cdot z_2 = 3x^3 + (4t+2)x^2 + (t^2 + 10t + 2)x + t^2 + 5t + 4,$$
$$z_2 \cdot z_1 = 3x^3 + (4t+1)x^2 + (t^2 + 11t + 4)x + t^2 + 4t + 3.$$

Example 4.1.3. Additive analogue of the Weyl algebra. $A_n(q_1, \dots, q_n)$ with $n = 2$ and $q_1 = q_2 = 2$.

Case I. Considering $A_2(2,2)$ as a skew PBW extension of $\mathbb{Q}$.

Let $A_2(2,2) = \sigma(\mathbb{Q})\langle x_1, x_2, y_1, y_2\rangle$, subject to relations (`rels`):

$$x_2x_1 = x_1x_2 \qquad y_2y_1 = y_1y_2$$
$$y_2x_1 = x_1y_2 \qquad y_1x_2 = x_2y_1$$

$$y_1x_1 = 2x_1y_1 + 1 \qquad y_2x_2 = 2x_2y_2 + 1.$$

The implementation of $A_2(2,2)$ is given by

$$A_2(2,2) := \texttt{SetSkewPBWExtension([}x_1, x_2, y_1, y_2\texttt{], rels,[}id, id, id, id\texttt{],[}0,0,0,0\texttt{]).}$$

Let $z_1 := y_1y_2^2$ and $z_2 := 3x_1^2x_2$, then

$$z_1 \cdot z_2 = 48x_1^2x_2y_1y_2^2 + 36x_1^2y_1y_2 + 36x_1x_2y_2^2 + 27x_1y_2.$$

Case II. Considering $A_2(2,2)$ as skew PBW extension of $\mathbb{Q}[x_1, x_2]$.

Let $A_2(2,2) = \sigma(\mathbb{Q}[x_1, x_2])\langle y_1, y_2\rangle$, subject to the relation (`rel`): $y_2y_1 = y_1y_2$. Here the σ_i's and the δ_i's must satisfy

$$\sigma_1(x_1) = q_1x_1, \quad \sigma_1(x_2) = x_2, \quad \sigma_2(x_1) = x_1, \quad \sigma_2(x_2) = q_2x_2;$$
$$\delta_1(x_1) = 1, \quad \delta_1(x_2) = 0, \quad \delta_2(x_1) = 0, \quad \delta_2(x_2) = 1.$$

Therefore,

$$\sigma_1(p) = \sum_j a_j q_1^{\alpha_j} x_1^{\alpha_j} x_2^{\beta_j}, \qquad \sigma_2(p) = \sum_j a_j q_2^{\beta_j} x_1^{\alpha_j} x_2^{\beta_j},$$
$$\delta_1(p) = \sum_j a_j \delta_1(x_1^{\alpha_j}) x_2^{\beta_j}, \qquad \delta_2(p) = \sum_j a_j x_1^{\alpha_j} \delta_2(x_2^{\beta_j}).$$

where $p = \sum_j a_j x_1^{\alpha_j} x_2^{\beta_j}$, and for $i = 1, 2$ we have

$$\delta_i(x_j^k) = \begin{cases} 0, & \text{if } i \neq j, \\ kx_i^{k-1}, & \text{if } q_i = 1 \text{ and } i = j, \\ \frac{1-q_i^k}{1-q_i} x_i^{k-1}, & \text{if } q_i \neq 1 \text{ and } i = j. \end{cases}$$

The implementation of $A_2(2,2)$ is given by

$$A_2(2,2) := \texttt{SetSkewPBWExtension([}y_1, y_2\texttt{],rel,[}\sigma_1, \sigma_2\texttt{],[}\delta_1, \delta_2\texttt{]),}$$

and again we get

$$z_1 \cdot z_2 = 48x_1^2x_2y_1y_2^2 + 36x_1^2y_1y_2 + 36x_1x_2y_2^2 + 27x_1y_2.$$

Example 4.1.4. Multiplicative analogue of the Weyl algebra. $\mathcal{O}_n(\lambda_{ji})$, with $n = 3$, $\lambda_{31} = 2$, $\lambda_{32} = 2$ and $\lambda_{21} = -1$.

Case I. Interpreting $\mathcal{O}_3(\lambda_{ji})$ as skew PBW extension of $\mathbb{Q}$.

Let $\mathcal{O}_3(\lambda_{ji}) = \sigma(\mathbb{Q})\langle x_1, x_2, x_3\rangle$, subject to relations (`rels`):

$x_3x_1 = 2x_1x_3, \quad x_3x_2 = 2x_2x_3, \quad x_2x_1 = -x_1x_2.$

The implementation of $\mathcal{O}_3(\lambda_{ji})$ is given by

$$\mathcal{O}_3(\lambda_{ji}) := \texttt{SetSkewPBWExtension(}[x_1, x_2, x_3]\texttt{,rels,}[id, id, id]\texttt{,}[0, 0, 0]\texttt{)}.$$

Let $z_1 := x_2x_3^2$ and $z_2 := 5x_1^2$, then

$z_1 \cdot z_2 = 80x_1^2x_2x_3^2.$

Case II. Considering $\mathcal{O}_3(\lambda_{ji})$ as skew PBW extension of $\mathbb{Q}[x_3]$.

Let $\mathcal{O}_3(\lambda_{ji}) = \sigma(\mathbb{Q}[x_3])\langle x_1, x_2\rangle$, subject to the relation (`rel`): $x_2x_1 = -x_1x_2$. Here the σ_i's and the δ_i's must satisfy

$\sigma_1(x_3) = \frac{1}{2}x_3, \quad \sigma_2(x_3) = \frac{1}{2}x_3, \quad \delta_1 = \delta_2 = 0.$

The implementation of $\mathcal{O}_3(\lambda_{ji})$ is given by

$$\mathcal{O}_3(\lambda_{ji}) := \texttt{SetSkewPBWExtension(}[x_1, x_2]\texttt{,rel,}[\sigma_1, \sigma_2]\texttt{,}[0, 0]\texttt{)},$$

and again

$z_1 \cdot z_2 = 80x_1^2x_2x_3^2.$

Example 4.1.5. q-Heisenberg algebra. $H_n(q)$ with $n = 2$ and $q = 2$.
Let $H_2(2) = \sigma(\mathbb{Q})\langle x_1, x_2, y_1, y_2, z_1, z_2\rangle$, subject to relations (`rels`):

$x_2x_1 = x_1x_2,$	$y_2y_1 = y_1y_2,$	$z_2z_1 = z_1z_2,$
$y_2x_1 = x_1y_2,$	$y_1x_2 = x_2y_1,$	$z_2y_1 = y_1z_2,$
$z_1y_2 = y_2z_1,$	$z_2x_1 = x_1z_2,$	$z_1x_2 = x_2z_1,$
$y_1x_1 = 2x_1y_1,$	$y_2x_2 = 2x_2y_2,$	$z_1y_1 = 2y_1z_1,$
$z_2y_2 = 2y_2z_2,$	$z_1x_1 = \frac{1}{2}x_1z_1 + y_1,$	$z_2x_2 = \frac{1}{2}x_2z_2 + y_2.$

The implementation of $H_2(2)$ is given by

$$H_2(2) := \texttt{SetSkewPBWExtension(}[x_1, x_2, y_1, y_2, z_3, z_2]\texttt{,rels,}L_3\texttt{,}L_4\texttt{)}$$

where $L_3 = [id, id, id, id, id, id]$ and $L_4 = [0, 0, 0, 0, 0, 0]$. Let $w_1 := x_1x_2y_1y_2z_1z_2$ and $w_2 := x_2^2z_2^2$, then

$w_1 \cdot w_2 = x_1x_2^3y_1y_2z_1z_2^3 + 5x_1x_2^2y_1y_2^2z_1z_2^2.$

Example 4.1.6. Difussion algebra.
Let $A = \sigma(\mathbb{Q}[x_1, x_2, x_3])\langle D_1, D_2, D_3\rangle$, subject to relations (`rels`):

$$\begin{aligned} D_2D_1 &= D_1D_2 + x_2D_1 - x_1D_2, \\ D_3D_1 &= D_1D_3 + x_3D_1 - x_1D_3, \\ D_3D_2 &= D_2D_3 + x_3D_2 - x_2D_3. \end{aligned}$$

The implementation of A is given by

A:=`SetSkewPBWExtension(`$[D_1, D_2, D_3]$`,rels,`$[id, id, id]$`,`$[0, 0, 0]$`)`

Let $z_1 := x_1x_2D_1D_2 + x_3D_1D_3$ and $z_2 := D_2^2D_3^2$, then

$$z_1 \cdot z_2 = x_1x_2D_1D_2^3D_3^2 + x_3D_1D_2^2D_3^3 + 2x_3^2D_1D_2^2D_3^2 - 2x_2x_3D_1D_2D_3^3 - x_2x_3^2D_1D_2D_3^2 + x_2^2x_3D_1D_3^3.$$

Example 4.1.7. Witten algebra.
Consider the Witten algebra denoted

$$W(\xi) := W(\xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6, \xi_7),$$

and defined by

$$zx = \xi_1^{-1}xz - \tfrac{\xi_2}{\xi_1}x, \quad zy = \xi_3yz + \xi_4y, \quad yx = \xi_5xy + \xi_6z^2 + \xi_7z.$$

Under certain conditions on the parameters, $W(\xi)$ is a skew PBW extension of $\mathbb{Q}$; consider the following particular example: $A = \sigma(\mathbb{Q})\langle x, y, z\rangle = W(\xi) = W(1, 1, 1, 2, 2, 0, 0)$ subject to relations (`rels`):

$$zx = xz - x, \quad zy = yz + 2y, \quad yx = 2xy.$$

The implementation of A is given by

A:=`SetSkewPBWExtension(`$[x, y, z]$`,rels,[id,id,id],[0,0,0])`.

Let $z_1 := z$, $z_2 := y + z^2$ and $z_3 := x - 2y$, then

$$(z_1 \cdot z_2) \cdot z_3 = xz^3 - 2yz^3 + 2xyz - 3xz^2 - 2y^2z - 12yz^2 + 2xy + 3xz - 8y^2 - 24yz - x - 16y = z_1 \cdot (z_2 \cdot z_3).$$

4.1.2. Division algorithm for left ideals

A fundamental function in the `SPBWEGrobner` package is the Division Algorithm for skew PBW extensions.

Division algorithm in A

INPUT: $f, f_1, \ldots, f_t \in A$ with $f_j \neq 0\,(1 \leq j \leq t)$

OUTPUT: $q_1, \ldots, q_t, h \in A$ with $f = q_1 f_1 + \cdots + q_t f_t + h$, h reduced w.r.t. $\{f_1, \ldots, f_t\}$ and

$$lm(f) = \max\{lm(lm(q_1)lm(f_1)), \ldots, lm(lm(q_t)lm(f_t)), lm(h)\} \tag{4-2}$$

INITIALIZATION: $q_1 := 0, q_2 := 0, \ldots, q_t := 0, h := f$

WHILE $h \neq 0$ and there exists j such that $lm(f_j)$ divides $lm(h)$ ***DO***

Calculate $J := \{j \mid lm(f_j) \text{ divides } lm(h)\}$

FOR $j \in J$ **DO**

Calculate $\alpha_j \in \mathbb{N}^n$ such that $\alpha_j + \exp(lm(f_j)) = \exp(lm(h))$

IF the equation

$$lc(h) = \sum_{j \in J} r_j \sigma^{\alpha_j}(lc(f_j)) c_{\alpha_j, f_j} \tag{4-3}$$

is soluble, where c_{α_j, f_j} are defined as in the Theorem 1.3.8 **THEN**

Calculate one solution $(r_j)_{j \in J}$

$h := h - \sum_{j \in J} r_j x^{\alpha_j} f_j$

FOR $j \in J$ **DO**

$q_j := q_j + r_j x^{\alpha_j}$

ELSE

Stop

Remark 4.1.8. The Euclidean Algorithm over commutative multivariate polynomial ring with coefficients in a field was used for the effective solution of the equation (4-3) in the implementation of Division Algorithm; in addition, it was used also the package `Grobner` of libraries inner of Maple. Therefore, the implementation of Division Algorithm, Buchberger's Algorithm and other algorithms below is feasible for skew PBW extensions, where the ring of coefficients is a commutative multivariate polynomial ring over a field, using existent libraries in Maple.

The statement for calling the Division Algorithm is:

```
DivisionAlgorithm(f,[f_1,...,f_n],order over A,skew PBW extension A)
```

Example 4.1.9. Taking the skew PBW extension $A := A_2(2,2)$ of Example 4.1.3 Case I, we can illustrate the use of `DivisionAlgorithm`:
Let $f := x_1x_2^2y_1^2y_2 + x_1^2x_2y_1$, $f_1 := x_1^2x_2y_1y_2$, $f_2 := x_2y_1$ and $f_3 := x_1y_2$. Then in this case `DivisionAlgorithm(`f`,[`f_1, f_2, f_3`],gradlex,`A`)` produces $q_1 = q_3 = 0$, $q_2 = \frac{1}{2}x_1x_2y_1y_2 + x_1^2 - \frac{1}{2}x_1y_1$ and $h = 0$, such that $f = q_1f_1 + q_2f_2 + q_3f_3 + h$, with h reduced and satisfying equation (4-2).

Example 4.1.10. Consider the difussion algebra $A := \sigma(\mathbb{Q}[x_1, x_2])\langle D_1, D_2\rangle$, subject to relation (`rel`)

$$D_2D_1 = 2D_1D_2 + x_2D_1 - x_1D_2.$$

Given $f := x_1x_2^2D_1^2D_2 + x_1^2x_2D_2$, $f_1 := x_1x_2D_1D_2$, $f_2 := x_2D_1$, $f_3 := x_1D_2$. Using the division algorithm `DivisionAlgorithm(`f`,[`f_1, f_2, f_3`],lex,`A`)` we get $q_1 := x_2D_1$, $q_2 := 0$, $q_3 := x_1x_2$ and $h = 0$. So, $f = q_1f_1 + q_2f_2 + q_3f_3 + h$, with h reduced and satisfying the equation (4-2).

4.1.3. Buchberger's algorithm for left ideals

Now we present the Maple implementation of the Buchberger's algorithm for the computation of left ideals of bijective skew PBW extension A.

Theorem 4.1.11. *Let $F = \{f_1, \ldots, f_s\}$ be a set of non-zero polynomials of A. The algorithm below produces a Gröbner basis for the left ideal $\langle F\}$ of A ($P(X)$ is the set of subsets of the set X):*

Buchberger's algorithm *in* A

INPUT: $F := \{f_1, \dots, f_s\} \subseteq A$, $f_i \neq 0$, $1 \leq i \leq s$

OUTPUT: $G = \{g_1, \dots, g_t\}$ *a Gröbner basis for* $\langle F\}$

INITIALIZATION: $G := \emptyset, G' := F$

WHILE $G' \neq G$ ***DO***

$D := P(G') - P(G)$

$G := G'$

FOR *each* $S := \{g_{i_1}, \dots, g_{i_k}\} \in D$ ***DO***

Compute B_S

FOR *each* $\boldsymbol{b} = (b_1, \dots, b_k) \in B_S$ ***DO***

Reduce $\sum_{j=1}^{k} b_j x^{\gamma_j} g_{i_j} \xrightarrow{G'}_+ r$, *with* r *reduced with respect to* G' *and* γ_j *defined as in Definition 1.4.6*

IF $r \neq 0$ ***THEN***

$G' := G' \cup \{r\}$

The statement for the Buchberger's Algorithm in the implementation is as follows:

`BuchbergerAlgSkewPoly(`L, ord, A`)`

`L` := List with the generators of the left ideal.
`ord` := Monomial order over A.

Example 4.1.12. Take the extension $A := A_2(2, 2)$ of Example 4.1.3 Case I.
The implementation of Buchberger Algorithm to find a Gröbner basis of $I := \langle f_1, f_2\}$, with $f_1 := x_1^2 x_2 y_1 y_2$ and $f_2 = x_2 y_1 + x_2$, is given by

`BuchbergerAlgSkewPoly([`f_1`,`f_2`],gradlex,`A`).`

The results is $G := \{g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8\}$, where

$$\begin{aligned}
g_1 &= x_1^2x_2y_1y_2,\\
g_2 &= x_2y_1 + x_2,\\
g_3 &= -6x_2^2y_2 - 3x_2y_1 - 3x_2,\\
g_4 &= -6x_1x_2^2y_2 - 3x_1x_2y_1 - 3x_1x_2,\\
g_5 &= -12x_2^2y_2^2 - 9x_2y_2,\\
g_6 &= -12x_1x_2^2y_2^2 - 9x_1x_2y_2,\\
g_7 &= -4x_1^2y_1^2 - 4x_1^2y_1 - 6x_1x_2y_2 - 3x_1y_1 - 3x_1,\\
g_8 &= -2x_1^2x_2y_2 - x_1^2y_1 - x_1^2.
\end{aligned}$$

Example 4.1.13. Consider $A := \mathcal{O}_3(2, 2, 2) = \sigma(\mathbb{Q})\langle x_1, x_2, x_3\rangle$ subject to relations:

$$x_3x_1 = 2x_1x_3, \quad x_3x_2 = 2x_2x_3, \quad x_2x_1 = 2x_1x_2.$$

For $I := \langle f_1, f_2\}$, with $f_1 := -x_1x_3 + x_1 + x_2$ and $f_2 = -x_2x_3 + x_3 + 1$, we have

`BuchbergerAlgSkewPoly(`$[f_1,f_2]$`,gradlex,`A`)`,

and the computed Gröbner basis for I is $G = \{g_1, g_2, g_3, g_4, g_5, g_6\}$, where

$$g_1 = 8x_3^2 + 24x_3 + 16, \qquad g_2 = 8x_2 + 8x_3 + 8, \qquad g_3 = 8x_1 + 4x_2,$$
$$g_4 = 2x_1x_2 - 2x_1x_3 + x_2^2 - 2x_1, \qquad g_5 = -x_1x_3 + x_1 + x_2, \qquad g_6 = -x_2x_3 + x_3 + 1.$$

Example 4.1.14. Consider the extension $A := H_2(2)$ of Example 4.1.5. The implementation of Buchberger Algorithm to find a Gröbner basis of $I := \langle f_1, f_2, f_3\}$, with $f_1 := x_1x_2y_1y_2$, $f_2 = x_2y_1$, $f_3 := y_2z_2$ and $f_4 := x_1 - y_1$, is given by

`BuchbergerAlgSkewPoly(`$[f_1, f_2, f_3]$`,lex,`A`)`.

The result is $G = \{g_1, g_2, g_3, g_4, g_5, g_6\}$, where

$$g_1 = x_1x_2y_1y_2, \quad g_2 = x_2y_1, \quad g_3 = y_2z_2,$$
$$g_4 = y_1y_2^2, \quad g_5 = y_1y_2^2, \quad g_6 = \tfrac{1}{2}y_1^2y_2^2.$$

Example 4.1.15. Take the Witten algebra $A := \sigma(\mathbb{Q})\langle x, y, z\rangle$ of Example 4.1.7. Consider $I := \langle f_1, f_2, f_3, f_4\}$, with $f_1 := x - y$, $f_2 = y + z$, $f_3 := 2x + 3y - z$ and $f_4 := xy$, so in this case we have

`BuchbergerAlgSkewPoly(`$[f_1, f_2, f_3, f_4]$`,gradlex,`A`)`,

and the Gröbner basis for I is $G = \{g_1, g_2, g_3, g_4, g_5, g_6\}$, where

$$g_1 = z^2 - 2x - 2y, \qquad g_2 = 6z, \qquad g_3 = x - y,$$
$$g_4 = y + z, \qquad g_5 = 2x + 3y - z, \qquad g_6 = xy.$$

4.1.4. Division algorithm for modules

Next we present the Division Algorithm for submodules of A^m, where A is a bijective skew PBW extension.

Theorem 4.1.16. *Let $F = \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_t\}$ be a set of non-zero vectors of A^m and $\boldsymbol{f} \in A^m$, then the Division Algorithm below produces polynomials $q_1, \ldots, q_t \in A$ and a reduced vector $\boldsymbol{h} \in A^m$ w.r.t.. F such that $\boldsymbol{f} \xrightarrow{F}_+ \boldsymbol{h}$ and*

$$\boldsymbol{f} = q_1\boldsymbol{f}_1 + \cdots + q_t\boldsymbol{f}_t + \boldsymbol{h}$$

with

$$lm(\boldsymbol{f}) = \max\{lm(lm(q_1)lm(\boldsymbol{f}_1)), \ldots, lm(lm(q_t)lm(\boldsymbol{f}_t)), lm(\boldsymbol{h})\}.$$

Division Algorithm in A^m

INPUT: $\boldsymbol{f}, \boldsymbol{f}_1, \dots, \boldsymbol{f}_t \in A^m$ *with* $\boldsymbol{f}_j \neq 0\,(1 \leq j \leq t)$

OUTPUT: $q_1, \dots, q_t \in A$, $\boldsymbol{h} \in A^m$ *with* $\boldsymbol{f} = q_1\boldsymbol{f}_1 + \cdots + q_t\boldsymbol{f}_t + \boldsymbol{h}$, $\boldsymbol{h}$ *reduced w.r.t..* $\{\boldsymbol{f}_1, \dots, \boldsymbol{f}_t\}$ *and*

$$lm(\boldsymbol{f}) = \max\{lm(lm(q_1)lm(\boldsymbol{f}_1)), \dots, lm(lm(q_t)lm(\boldsymbol{f}_t)), lm(\boldsymbol{h})\}. \qquad (4\text{-}4)$$

INITIALIZATION: $q_1 := 0, q_2 := 0, \dots, q_t := 0, \boldsymbol{h} := \boldsymbol{f}$

WHILE $\boldsymbol{h} \neq \boldsymbol{0}$ *and there exists* j *such that* $lm(\boldsymbol{f}_j)$ *divides* $lm(\boldsymbol{h})$ **DO**

Calculate $J := \{j \,|\, lm(\boldsymbol{f}_j) \text{ divides } lm(\boldsymbol{h})\}$

FOR $j \in J$ ***DO***

Calculate $\alpha_j \in \mathbb{N}^n$ *such that* $\alpha_j + \exp(lm(\boldsymbol{f}_j)) = \exp(lm(\boldsymbol{h}))$

IF *the equation* $lc(\boldsymbol{h}) = \sum_{j\in J} r_j \sigma^{\alpha_j}(lc(\boldsymbol{f}_j))c_{\alpha_j,\boldsymbol{f}_j}$ *is soluble, where* $c_{\alpha_j,\boldsymbol{f}_j}$ *are defined as in Definition 1.4.15*

THEN

Calculate one solution $(r_j)_{j\in J}$

$\boldsymbol{h} := \boldsymbol{h} - \sum_{j\in J} r_j x^{\alpha_j}\boldsymbol{f}_j$

FOR $j \in J$ ***DO***

$q_j := q_j + r_j x^{\alpha_j}$

ELSE

Stop

In this case the implementation for the Division Algorithm is as follows:

`DivisionAlgorithm(`$L, \text{ord}, \text{ORD}, A$`)`

`L`	:= List with generators of the submodule.
`ord`	:= Monomial order over A.
`ORD`	:= Order over A^m.

Let $\boldsymbol{f} \neq \boldsymbol{0}$ be a vector of A^m, the next function is a very useful tool for working in A^m: We fix a monomial order on $Mon(A)$, then we may write $\mathbf{f}$ as a sum of terms; using the statement `PrintSkewPolyVector(f,vars,ord,ORD)`, we get an ordered list of terms which adds $\mathbf{f}$.

`vars`	:= variables $x_1, \dots, x_n$, assuming $x_1 \succ \cdots \succ x_n$.
`ord`	:= Monomial order over A.
`ORD`	:= Order over A^m.

Example 4.1.17. Let $A := \sigma(R)\langle x, y\rangle$ be a skew PBW extension and let $\mathbf{f} := (6x^2y^3 + 2xy^4 - x^3y + 3x^2 + xy, -6x^3y^5 + 5x^2y^4 + 2x^3 + 3x^2y + xy^2, 5x^4y^4 + 3x^3y^5 - xy) \in A^3$. Using the statement `PrintSkewPolyVector(f,[x,y],lex,TOPREV))`. We get

$$\mathbf{f} = 5x^4y^4\boldsymbol{e}_3 - 6x^3y^5\boldsymbol{e}_2 + 3x^3y^5\boldsymbol{e}_3 + -x^3y\boldsymbol{e}_1 + 2x^3\boldsymbol{e}_2 + 5x^2y^4\boldsymbol{e}_2 + \\ + 6x^2y^3\boldsymbol{e}_1 + 3x^2y\boldsymbol{e}_2 + 3x^2\boldsymbol{e}_1 + 2xy^4\boldsymbol{e}_1 + xy^2\boldsymbol{e}_2 + xy\boldsymbol{e}_1 - xy\boldsymbol{e}_3.$$

For other useful tools for making computations with vectors in A^m see Appendix A.

Example 4.1.18. Take the extension $A := H_1(2)$, i.e., $A := \sigma(\mathbb{Q})\langle x, y, z\rangle$, subject to relations (`rels`):

$$yx = 2xy, \quad zx = \tfrac{1}{2}xz + y, \quad zy = 2yz.$$

Given $\mathbf{f} := (x^2yz + xz, y^2z, z^2)$, $\mathbf{f}_1 := (xz, y, x)$ and $\mathbf{f}_2 := (xy, z, z)$, the Division Algorithm `DivisionAlgorithm(f, [f`$_1$`,f`$_2$`,f`$_3$`],gradlex,TOPREV,`A`)` produces $q_1 := \frac{1}{2}xy$, $q_2 := 0$ and $\mathbf{h} = (xz, y^2z - \frac{1}{2}xy^2, z^2 - x^2y)$. So, $\mathbf{f} = q_1\mathbf{f}_1 + q_2\mathbf{f}_2 + \mathbf{h}$, with $\mathbf{h}$ reduced, and satisfies the equation (4-4).

Example 4.1.19. Consider the difussion algebra $A := \sigma(\mathbb{Q}[x_1, x_2])\langle D_1, D_2\rangle$ subject to relation (`rel`):

$$D_2D_1 = 2D_1D_2 + x_2D_1 - x_1D_2.$$

Given the following vectors in A^2

$$\begin{aligned} \mathbf{f} &:= ((x_1x_2 + 1)D_1^2D_2^2 + x_1D_1^2, x_2D_2^2 + D_1D_2), \\ \mathbf{f}_1 &:= (x_1D_1D_2 + x_1D_1, D_2^2), \\ \mathbf{f}_2 &:= (D_1D_2^2, D_1^2 + x_1D_1D_2), \\ \mathbf{f}_3 &:= (D_2, D_1^2), \\ \mathbf{f}_4 &:= (x_1D_1, D_2^2 + x_2), \end{aligned}$$

we apply the Division Algorithm:

`DivisionAlgorithm(f,[f`$_1$`,f`$_2$`,f`$_3$`,f`$_4$`],gradlex,TOPREV,`A`)`

and we obtain

$$q_1 = \tfrac{1}{2}x_2D_1D_2 - \tfrac{1}{2}x_2^2D_1 + \tfrac{1}{4}x_1x_2D_2, \qquad q_2 = D_1,$$
$$q_3 = -D_1 - \tfrac{1}{4}x_1D_2, \qquad q_4 = -\tfrac{1}{2}x_2D_1D_2 + \tfrac{1}{2}x_2^2D_1 - \tfrac{1}{4}x_1x_2D_2,$$

$$\mathbf{h} = (x_1D_1^2 + (1 - \tfrac{1}{4}x_1^2x_2^2)D_1D_2 + (\tfrac{1}{4}x_1 + \tfrac{1}{4}x_1^3x_2)D_2^2)\boldsymbol{e}_1 + \\ ((1 + \tfrac{1}{2}x_2^2 - x_1^2)D_1D_2 + x_2D_2^2 + \tfrac{3}{4}x_1x_2D_1^2 + (-\tfrac{1}{4}x_1^2x_2 - \tfrac{1}{2}x_2^3)D_1 + (\tfrac{1}{4}x_1^3 + \tfrac{1}{4}x_1x_2^2)D_2)\boldsymbol{e}_2.$$

Note that $\mathbf{f} = q_1\mathbf{f}_1 + q_2\mathbf{f}_2 + q_3\mathbf{f}_3 + q_4\mathbf{f}_4 + \mathbf{h}$, with $\mathbf{h}$ reduced and satisfying the equation (4-4).

4.1.5. Buchberger's algorithm for modules

We conclude this section with the Maple implementation of the Buchberger's Algorithm for computing the Gröbner bases of submodules of A^m, where A is a bijective skew PBW extension.

Theorem 4.1.20. *Let $F = \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\}$ be a set of non-zero vectors of A^m. The algorithm below produces a Gröbner basis for the submodule $\langle \boldsymbol{f}_1, \ldots, \boldsymbol{f}_s \rangle$ ($P(X)$ is the set of subsets of the set X):*

> ***Buchberger's algorithm in*** A^m
>
> ***INPUT***: $F := \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\} \subseteq A^m$, $\boldsymbol{f}_i \neq \boldsymbol{0}$, $1 \leq i \leq s$
>
> ***OUTPUT***: $G = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_t\}$ *a Gröbner basis for* $\langle F \rangle$
>
> ***INITIALIZATION***: $G := \emptyset, G' := F$
>
> ***WHILE*** $G' \neq G$ ***DO***
>
> $D := P(G') - P(G)$
>
> $G := G'$
>
> ***FOR*** *each* $S := \{\boldsymbol{g}_{i_1}, \ldots, \boldsymbol{g}_{i_k}\} \in D$, *with* $\boldsymbol{X}_S \neq \boldsymbol{0}$, ***DO***
>
> *Compute* B_S
>
> ***FOR*** *each* $\boldsymbol{b} = (b_1, \ldots, b_k) \in B_S$ ***DO***
>
> *Reduce* $\sum_{j=1}^{k} b_j x^{\gamma_j} \boldsymbol{g}_{i_j} \xrightarrow{G'}_{+} \boldsymbol{r}$, *with* $\boldsymbol{r}$ *reduced with respect to* G' *and* γ_j *defined as in Definition 1.4.19*
>
> ***IF*** $\boldsymbol{r} \neq \boldsymbol{0}$ ***THEN***
>
> $G' := G' \cup \{\boldsymbol{r}\}$

The statement for the Buchberger's Algorithm in the implementation is as follows:

`BuchbergerAlgSkewPoly(`$L, \mathrm{ord}, \ \mathrm{ORD}, A$`)`

`L` := List with the generators of the submodule.
`ord` := Monomial order over A.
`ORD` := Order over A^m.

Example 4.1.21. Consider the additive analogue of the Weyl algebra $A = A_2(\frac{1}{2}, \frac{1}{3})$. Let $\boldsymbol{f}_1 = x_1 y_1^2 \boldsymbol{e}_1 + x_2 y_2 \boldsymbol{e}_2$ and $\boldsymbol{f}_2 = x_2 y_2^2 \boldsymbol{e}_1 + x_1 y_1 \boldsymbol{e}_2$. We will construct a Gröbner basis for the module $M := \langle \boldsymbol{f}_1, \boldsymbol{f}_2 \rangle$. Recall that $A = \sigma(\mathbb{Q}[x_1, x_2])\langle y_1, y_2 \rangle$ is subjected to relations (`rels`):

$$y_1 x_1 = \tfrac{1}{2} x_1 y_1 + 1, \ y_2 x_2 = \tfrac{1}{3} x_2 y_2 + 1, \ x_1 y_2 = y_2 x_1, \ x_2 y_1 = y_1 x_2, \ y_1 y_2 = y_2 y_1.$$

Then, we apply `BuchbergerAlgSkewPoly([f`$_1$`,f`$_2$`],gradlex,TOPREV,`A`)` and we get the Gröbner basis $G=\{\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3\}$, where

$$\mathbf{g}_1=x_1y_1^2\boldsymbol{e}_1+x_2y_2\boldsymbol{e}_2,\quad \mathbf{g}_2=x_2y_2^2\boldsymbol{e}_1+x_1y_1\boldsymbol{e}_2,\quad \mathbf{g}_3=-\tfrac{1}{4}x_1^2y_1^3\boldsymbol{e}_2+\tfrac{1}{9}x_2^2y_2^3\boldsymbol{e}_2-\tfrac{3}{2}x_1y_1^2\boldsymbol{e}_2+\tfrac{4}{3}x_2y_2^2\boldsymbol{e}_2.$$

Example 4.1.22. For $A:=\mathcal{O}_3(2,\frac{1}{2},3)=\sigma(\mathbb{Q})\langle x_1,x_2,x_3\rangle$ the relations (`rels`) are:

$$x_2x_1=2x_1x_2,\quad x_3x_1=\tfrac{1}{2}x_1x_3,\quad x_3x_2=3x_2x_3.$$

Let $M:=\langle f_1,f_2\rangle$, with $\mathbf{f}_1:=x_1^2x_2^2\boldsymbol{e}_1+x_2x_3\boldsymbol{e}_2$ and $\mathbf{f}_2:=2x_1x_2x_3\boldsymbol{e}_1+x_2\boldsymbol{e}_2$. We calculate `BuchbergerAlgSkewPoly([f`$_1$`,f`$_2$`],gradlex,TOPREV,`$A$`)` and we obtain $G=\{\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3\}$, where

$$\mathbf{g}_1=48x_2x_3^2\boldsymbol{e}_2-9x_1x_2^2\boldsymbol{e}_2,\quad \mathbf{g}_2=x_1^2x_2^2\boldsymbol{e}_1+x_2x_3\boldsymbol{e}_2,\quad \mathbf{g}_3=2x_1x_2x_3\boldsymbol{e}_1+x_2\boldsymbol{e}_2.$$

Example 4.1.23. Let $A:=\sigma(\mathbb{Q}[x])\langle y,z,w\rangle$ subjected to relationes (`rels`):

$$yx=\tfrac{3}{2}xy,\qquad wx=\tfrac{2}{3}xw,\qquad zy=\tfrac{2}{3}yz,\qquad wz=\tfrac{2}{3}zw$$
$$zx=xz,\qquad wy=yw-\tfrac{5}{6}xz,$$

Note that

$$\sigma_1(x)=\tfrac{3}{2}x,\quad \sigma_2(x)=x \text{ and } \sigma_3(x)=\tfrac{2}{3}x.$$

Let $\boldsymbol{f}_1=xyw\boldsymbol{e}_1+w\boldsymbol{e}_2$ and $\boldsymbol{f}_2=x^2zw\boldsymbol{e}_1+xy\boldsymbol{e}_2$. Then, a Gröbner basis for $M:=\langle\boldsymbol{f}_1,\boldsymbol{f}_2\rangle$, using `BuchbergerAlgSkewPoly([f`$_1$`,f`$_2$`],gradlex,TOPREV,`$A$`)`, is: $G=\{\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3\}$, whe-re

$$\mathbf{g}_1=xyw\boldsymbol{e}_1+w\boldsymbol{e}_2,\quad \mathbf{g}_2=x^2zw\boldsymbol{e}_1+xy\boldsymbol{e}_2,\quad \mathbf{g}_3=-12xy^2\boldsymbol{e}_2+27xzw\boldsymbol{e}_2.$$

4.2. Some homological computations

4.2.1. Computation of syzygies

Now we will implement in Maple an algorithm that computes the syzygy module of a finite set of polynomials of A, and more generally, of a finite set of elements of A^m.

Syzygy module algorithm in A^m

INPUT: $M := [\mathbf{f}_1 \ \cdots \ \mathbf{f}_s]^T \in \mathcal{M}_{s\times m}(A)$ with $\mathbf{f}_i \in A^m$, $1 \le i \le s$

OUTPUT: Matrix, where its rows are generators of $Syz_A(M)$.

STEP 1: Apply the Buchberger's algorithm to find a Gröbner basis G of $F := \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\} \subseteq A^m$.

STEP 2: Find matrices H^T and Q^T of Theorem 1.4.8 (for modules).

STEP 3: Find $Z(G)$ using the Theorem 1.4.25.

STEP 4: Compute $Syz(F)$ = eliminating some dependent rows of $[(Z(G)^T H^T)^T \quad (I_s - Q^T H^T)^T]^T$.

RETURN: $Syz(F)$.

The statement that computes syzygy of a finite set $F := \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\} \subseteq A^m$ is as follows:

$$\texttt{SyzModule(}M, \text{ord}, \ \text{ORD}, A\texttt{)},$$

where M is a matrix which rows are the elements $\boldsymbol{f}_1^T, \ldots, \boldsymbol{f}_s^T$. Calling this statement, it returns a matrix which rows are the generators of $Syz(F)$. Note that if $m = 1$, the algorithm computes the syzygy ideal.

Example 4.2.1. Consider the diffusion algebra $A := \sigma(\mathbb{Q}[x_1, x_2])\langle D_1, D_2\rangle$ subject to relation (`rel`):

$$D_2D_1 = 2D_1D_2 + x_2D_1 - x_1D_2,$$

we want to find a finite set of generators for $Syz(f_1, f_2)$, where $f_1 = x_1^2x_2D_1^2D_2$ and $f_2 = x_2^2D_1D_2^2$. Let $M := [f_1 \quad f_2]^T$, applying `SyzModule(`M`, gradlex, TOPREV, `A`)`, we get a Gröbner basis

$$G = [x_1^2x_2D_1^2D_2, x_2^2D_1D_2^2, -x_1^3x_2^3D_1D_2, x_1^4x_2^2D_2^2, -x_1^3x_2^4D_1D_2 + x_1^4x_2^3D_2^2 + x_1^4x_2^2D_2^3],$$

$$H^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ x_2D_2 - 3x_2^2 & -4x_1^2D_1 + 4x_1^3 \\ x_2D_2^2 - 3x_2^2D_2 & -8x_1^2D_1D_2 - 4x_1^2x_2D_1 + 8x_1^3D_2 + 2x_2x_1^3 \end{bmatrix}, \ Q^T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

$Z(G) = \langle \boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3, \boldsymbol{s}_4, \boldsymbol{s}_5, \boldsymbol{s}_6, \boldsymbol{s}_7, \boldsymbol{s}_8, \boldsymbol{s}_9, \boldsymbol{s}_{10}, \boldsymbol{s}_{11}\rangle$ where,

$$
\begin{aligned}
\boldsymbol{s}_1 &= (x_1x_2^2, -x_1^4, D_1, 0),\\
\boldsymbol{s}_2 &= (0, 2x_1^3x_2, D_2, -1),\\
\boldsymbol{s}_3 &= (x_2^3x_1, 2x_1^3x_2D_1 - \tfrac{1}{2}x_1^4D_2 - \tfrac{1}{2}x_1^4x_2, D_1D_2 + \tfrac{1}{2}x_1x_2, -\tfrac{1}{2}x_1),\\
\boldsymbol{s}_4 &= (x_2D_2 - 3x_2^2, -4x_1^2D_1 + 4x_1^3, -1, 0),\\
\boldsymbol{s}_5 &= (4x_1x_2^4, -2x_1^4x_2^2, x_1D_2^2 + 2x_1x_2^2, 4x_2D_1 - x_1D_2 - 2x_1x_2),\\
\boldsymbol{s}_6 &= (0, 2x_2x_1^3D_2, D_2^2, -D_2),\\
\boldsymbol{s}_7 &= (-2x_2^3x_1, x_1^4D_2 + x_1^4x_2, -x_1x_2, -2D_1 + x_1),\\
\boldsymbol{s}_8 &= (4x_2^4x_1D_1 + x_1^2x_2^4, -\tfrac{1}{4}x_1^5D_2^2 - x_1^5x_2D_2 - \tfrac{5}{4}x_1^5x_2^2, x_1D_1D_2^2 + \tfrac{5}{4}x_1^2x_2^2,\\
&\qquad 4x_2D_1^2 - \tfrac{3}{4}x_1^2D_2 - \tfrac{1}{2}x_1^2x_2),\\
\boldsymbol{s}_9 &= (\tfrac{1}{2}x_2^3x_1D_2 - \tfrac{1}{2}x_2^4x_1, 2x_2x_1^3D_1D_2 - \tfrac{1}{4}x_1^4D_2^2 - \tfrac{1}{4}x_1^4x_2^2, D_1D_2^2 - \tfrac{1}{4}x_1x_2^2,\\
&\qquad -\tfrac{3}{4}x_1D_2 + \tfrac{1}{2}x_1x_2),\\
\boldsymbol{s}_{10} &= (-2x_2^3x_1D_1 + \tfrac{1}{4}x_1^2x_2^2D_2 - \tfrac{3}{4}x_1^2x_2^3, x_1^4D_1D_2 + \tfrac{1}{2}x_1^5D_2 + \tfrac{1}{2}x_1^5x_2, -\tfrac{3}{4}x_1^2x_2, -2D_1^2 + \tfrac{1}{2}x_1^2),\\
\boldsymbol{s}_{11} &= (x_2D_2^2 - 4x_2^2D_2 + 3x_2^3, -8x_1^2D_1D_2 + 8x_1^3D_2 - 2x_2x_1^3, x_2, -1).
\end{aligned}
$$

The implementation returns

$$Syz(F) = \langle (x_2D_1D_2 - 3x_2^2D_1 + x_1x_2^2)\boldsymbol{e}_1 + (-4x_1^2D_1^2 + 4x_1^3D_1 - x_1^4)\boldsymbol{e}_2\rangle.$$

Example 4.2.2. Take the Witten's algebra $A := \sigma(\mathbb{Q})\langle x, y, z\rangle$ subject to relations

$$zx = xz - x, \quad zy = yz + 2y \quad yx = -xy.$$

We want to find a finite set of generators for the submodule $Syz(\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3)$ of A^2, where $\boldsymbol{f}_1 = \boldsymbol{e}_1 + (x+y)\boldsymbol{e}_2$, $\boldsymbol{f}_2 = z\boldsymbol{e}_2$, $\boldsymbol{f}_3 = y\boldsymbol{e}_1 + xz\boldsymbol{e}_2$. Let $M := [\boldsymbol{f}_1^T \ \boldsymbol{f}_2^T \ \boldsymbol{f}_3^T]^T$, applying `SyzModule(`$M$`, gradlex, TOPREV, `$A$`)`, we get a Gröbner basis $G = \{\boldsymbol{g}_1, \boldsymbol{g}_2, \boldsymbol{g}_3, \boldsymbol{g}_4, \boldsymbol{g}_5, \boldsymbol{g}_6, \boldsymbol{g}_7\}$, where

$$
\begin{aligned}
&\boldsymbol{g}_1 = \boldsymbol{e}_1 + (x+y)\boldsymbol{e}_2, \quad \boldsymbol{g}_2 = z\boldsymbol{e}_2, \quad \boldsymbol{g}_3 = y\boldsymbol{e}_1 + xz\boldsymbol{e}_2, \quad \boldsymbol{g}_4 = (z+1)\boldsymbol{e}_1 + 3y\boldsymbol{e}_2,\\
&\boldsymbol{g}_5 = (z - y + 1)\boldsymbol{e}_1 + 3y\boldsymbol{e}_2, \quad \boldsymbol{g}_6 = (3y + xz + x)\boldsymbol{e}_1 + 3y^2\boldsymbol{e}_2, \quad \boldsymbol{g}_7 = (-z^2 - z)\boldsymbol{e}_1 - 6y\boldsymbol{e}_2,
\end{aligned}
$$

$$
H^T = \begin{bmatrix} 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\\ z+1 & -x-y & 0\\ z+1 & -y & -1\\ xz+x+3y & -x^2-xy & 0\\ -z^2-z & xz+yz-x+5y & 0 \end{bmatrix}, \quad Q^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0\\ z+1 & -y & 0 & 0 & -1 & 0 & 0 \end{bmatrix},
$$

$Z(G) = \langle \boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3, \boldsymbol{s}_4, \boldsymbol{s}_5, \boldsymbol{s}_6, \boldsymbol{s}_7, \boldsymbol{s}_8, \boldsymbol{s}_9, \boldsymbol{s}_{10}, \boldsymbol{s}_{11}, \boldsymbol{s}_{12}\rangle$ where,

$\boldsymbol{s}_1 = (3y, 0, 0, x, 0, -1, 0),$
$\boldsymbol{s}_2 = (0, 3y, 0, -z, 0, 0, -1),$
$\boldsymbol{s}_3 = (3yz + 6y, -3y^2 - 3yz + 9y, 0, y^2 + 2y - 4, xz + yz + z^2 - x - 4y - 5z + 4, -y - z, z - 5),$
$\boldsymbol{s}_4 = (0, -3yz + 9y, 0, -2y - 4, z^2 - 5z + 4, 0, -y + z - 5),$
$\boldsymbol{s}_5 = (-6y, -3y^2, 0, -3y, 0, z + 1, x),$
$\boldsymbol{s}_6 = (0, x, -1, 1, -1, 0, 0),$
$\boldsymbol{s}_7 = (z + 1, -y, -1, 0, -1, 0, 0),$
$\boldsymbol{s}_8 = -6y^2 + 3yz + 6y, -3y^3 - 3y^2 - 3yz + 9y, 0, -2y^2 + 2y - 4, xz + yz + z^2 - x - 4y - 5z + 4,$
$yz - z, -xy + z - 5),$
$\boldsymbol{s}_9 = (3yz^2 - 6y^2 + 9yz + 6y, -6y^2 - 6yz + 18y, 0, 2y^2 + 4y - 8, xz^2 - 3xz + 2yz + 2z^2 + 2x-$
$8y - 10z + 8, -z^2 + z, -xy + 2z - 10),$
$\boldsymbol{s}_{10} = (6y, 3y^2, 3y, xz, 3y, -z - 1, 0),$
$\boldsymbol{s}_{11} = (-6y, 3xy - 3y^2, 0, -xz - 3y, 0, z + 1, 0),$
$\boldsymbol{s}_{12} = (3yz + 9y, 0, 0, xz, 0, -z - 1, 0).$

The implementation returns a matrix $L \in \mathcal{M}_{4\times 3}(A)$, with

$L_{11} = yz^2 - yz - 2y,$
$L_{12} = xyz + xz^2 - y^2z - 3xy - 7xz - 3y^2 + 10x,$
$L_{13} = -z^2 + 5z - 4,$
$L_{21} = xyz + y^2z + yz^2 + xy - 2y^2 - yz - 2y,$
$L_{22} = x^2y + x^2z - 2xy^2 + xz^2 - y^3 - y^2z - 2x^2 + 2xy - 7xz - 3y^2 + 10x,$
$L_{23} = -xz - yz - z^2 + x + 4y + 5z - 4.$

Therefore,

$$Syz(\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3) = \langle \boldsymbol{u}_1, \boldsymbol{u}_2\rangle, \text{ with } \boldsymbol{u}_i = L_{i1}\boldsymbol{e}_1 + L_{i2}\boldsymbol{e}_2 + L_{i3}\boldsymbol{e}_3 \text{ for } i = 1, 2.$$

Example 4.2.3. Considering the multiplicative analogue of the Weyl algebra. $A = \mathcal{O}_n(\lambda_{ji})$, with $n = 3$, $\lambda_{31} = 2$, $\lambda_{32} = 2$ and $\lambda_{21} = -1$. Then A is subject to relations:

$$x_3x_1 = 2x_1x_3, \quad x_3x_2 = 2x_2x_3, \quad x_2x_1 = -x_1x_2.$$

We want to find a finite set of generators for the submodule $Syz(\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3, \boldsymbol{f}_4, \boldsymbol{f}_5)$ of A^2, where $\boldsymbol{f}_1 = x_1\boldsymbol{e}_1 + (x_2 + 1)\boldsymbol{e}_2$, $\boldsymbol{f}_2 = x_3\boldsymbol{e}_1$, $\boldsymbol{f}_3 = \boldsymbol{e}_1 + x_2\boldsymbol{e}_2$, $\boldsymbol{f}_4 = x_2\boldsymbol{e}_1 + x_1x_3\boldsymbol{e}_2$ and $\boldsymbol{f}_5 = (x_3 - 1)\boldsymbol{e}_1$. Let $M := [\boldsymbol{f}_1^T\ \boldsymbol{f}_2^T\ \boldsymbol{f}_3^T\ \boldsymbol{f}_4^T\ \boldsymbol{f}_5^T]^T$, applying `SyzModule(`$M$`, gradlex, TOP,` A`)`, we get a Gröbner basis $G = \{\boldsymbol{g}_1, \boldsymbol{g}_2, \boldsymbol{g}_3, \boldsymbol{g}_4, \boldsymbol{g}_5, \boldsymbol{g}_6, \boldsymbol{g}_7, \boldsymbol{g}_8\}$, where

$\boldsymbol{g}_1 = x_1\boldsymbol{e}_1 + (x_2 + 1)\boldsymbol{e}_2,\ \boldsymbol{g}_2 = x_3\boldsymbol{e}_1, \quad \boldsymbol{g}_3 = \boldsymbol{e}_1 + x_2\boldsymbol{e}_2, \quad \boldsymbol{g}_4 = x_2\boldsymbol{e}_1 + x_1x_3\boldsymbol{e}_2,$
$\boldsymbol{g}_5 = (x_3 - 1)\boldsymbol{e}_1, \quad \boldsymbol{g}_6 = -x_3\boldsymbol{e}_1 + x_3\boldsymbol{e}_2, \quad \boldsymbol{g}_7 = 2\boldsymbol{e}_1 - 2\boldsymbol{e}_2, \quad \boldsymbol{g}_8 = \boldsymbol{e}_1,$

$$H^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ x_3 & -2x_1 & -x_3 & 0 & 0 \\ -2 & 2x_1 & 2 & 0 & -2x_1 \\ 0 & 1 & 0 & 0 & -1 \end{bmatrix}, \quad Q^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix},$$

$Z(G) = \langle \boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3, \boldsymbol{s}_4, \boldsymbol{s}_5, \boldsymbol{s}_6, \boldsymbol{s}_7, \boldsymbol{s}_8, \boldsymbol{s}_9, \boldsymbol{s}_{10}, \boldsymbol{s}_{11}, \boldsymbol{s}_{12}, \boldsymbol{s}_{13}, \boldsymbol{s}_{14}, \boldsymbol{s}_{15} \rangle$, where

$$\begin{aligned}
\boldsymbol{s}_1 &= (1, 0, -1, 0, 0, 0, \tfrac{1}{2}, -x_1), \\
\boldsymbol{s}_2 &= (0, 0, 2, 0, 0, 0, x_2, -2x_2 - 2), \\
\boldsymbol{s}_3 &= (0, 0, 0, 0, 0, 2, x_3, 0), \\
\boldsymbol{s}_4 &= (0, 0, 0, 0, 1, 0, 0, -x_3 + 1), \\
\boldsymbol{s}_5 &= (0, 1, 0, 0, 0, 0, 0, -x_3), \\
\boldsymbol{s}_6 &= (0, 0, 0, 0, 0, 2x_2, x_2x_3, 0), \\
\boldsymbol{s}_7 &= (0, -2x_2 - 1, x_3, 0, 0, 0, x_2x_3, 0), \\
\boldsymbol{s}_8 &= (0, 0, 0, 0, 0, 2x_1, x_1x - 3, 0), \\
\boldsymbol{s}_9 &= (-x_3, 0, x_3, 2, 0, 1, x_1x_3, -2x_2), \\
\boldsymbol{s}_{10} &= (1, 0, -1, 0, x_1, 0, \tfrac{1}{2}, -x_1x_3), \\
\boldsymbol{s}_{11} &= (0, x_1, 0, 0, 0, 0, 0, -x_1x_3), \\
\boldsymbol{s}_{12} &= (x_3, 0, -x_3, 0, 0, -1, 0, -2x_1x_3), \\
\boldsymbol{s}_{13} &= (0, 0, 0, 0, 0, 2x_1x_2, x_1x_2x_3, 0), \\
\boldsymbol{s}_{14} &= (-x_2x_3, -x_2 - \tfrac{1}{2}, x_2x_3 + \tfrac{1}{2}x_3, 2x_2, 0, 0, -x_1x_2x_3, -2x_2^2)), \\
\boldsymbol{s}_{15} &= (x_2x_3 - \tfrac{1}{2}x_3, x_2 + \tfrac{1}{2}, x_1x_3 - x_2x_3, 0, 0, \tfrac{1}{2}, x_1x_2x_3, 0).
\end{aligned}$$

Finally, the implementation return the matrix L with rows as generators, and we get

$Syz(\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3, \boldsymbol{f}_4, \boldsymbol{f}_5) = \langle \boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3, \boldsymbol{w}_4, \boldsymbol{w}_5, \boldsymbol{w}_6 \rangle$,

where

$$\begin{aligned}
\boldsymbol{w}_1 &= -2x_2\boldsymbol{e}_1 - (2x_1x_2 + 2x_2 + 2)\boldsymbol{e}_2 + (2x_2 + 2)\boldsymbol{e}_3 + (2x_1x_2 + 2x_2 + 2)\boldsymbol{e}_5, \\
\boldsymbol{w}_2 &= (-x_3 + 1)\boldsymbol{e}_2 + x_3\boldsymbol{e}_5, \\
\boldsymbol{w}_3 &= (-4x_1x_2x_3 + 4x_1x_2)\boldsymbol{e}_2 + 4x_1x_2x_3\boldsymbol{e}_5, \\
\boldsymbol{w}_4 &= -2x_1x_3\boldsymbol{e}_1 + (4x_1^2x_3 - 2x_1 - 2x_2)\boldsymbol{e}_2 + 2x_1x_3\boldsymbol{e}_3 + 2\boldsymbol{e}_4 + (-4x_1^2x_3 + 2x_2)\boldsymbol{e}_5, \\
\boldsymbol{w}_5 &= (-4x_1^2x_2x_3 + 4x_1^2x_2)\boldsymbol{e}_2 + 4x_1^2x_2x_3\boldsymbol{e}_5, \\
\boldsymbol{w}_6 &= (2x_1x_2x_3 - x_2x_3)\boldsymbol{e}_1 + (4x_1^2x_2x_3 - 2x_2^2 - x_2 - \tfrac{1}{2})\boldsymbol{e}_2 + (-2x_1x_2x_3 + x_2x_3 + \tfrac{1}{2}x_3)\boldsymbol{e}_3 + \\
&\quad 2x_2\boldsymbol{e}_4 + (-4x_1^2x_2x_3 + 2x_2^2)\boldsymbol{e}_5.
\end{aligned}$$

Example 4.2.4. We taking again the additive analogue of the Weyl algebra $A =: A_2(\frac{1}{2}, \frac{1}{3})$, we want to find a finite set of generators for the submodule $Syz(\boldsymbol{f}_1, \boldsymbol{f}_2)$ of A^2, where $\boldsymbol{f}_1 =$

$x_1y_1^2\boldsymbol{e}_1 + x_2y_2\boldsymbol{e}_2$ and $\boldsymbol{f}_2 = x_2y_2^2\boldsymbol{e}_1 + x_1y_1\boldsymbol{e}_2$. Let $M := [\boldsymbol{f}_1^T \;\; \boldsymbol{f}_2^T]^T$, applying `SyzModule(`$M$`, gradlex, TOPREV,` A`)`, we get a Gröbner basis G of Example 4.1.21,

$$H^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ x_2y_2^2 & -x_1y_1^2 \end{bmatrix}, \; Q^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \text{ and } Z(G) = [x_2y_2^2\boldsymbol{e}_1 - x_1y_1^2\boldsymbol{e}_2 - \boldsymbol{e}_3].$$

The implementation return: $Syz(M) = 0$, i.e., M is a free left module of rank 2.

4.2.2. Computation of free resolutions

Now we will implement in Maple an algorithm that computes a free resolution of a a given submodule of A^m.

Free resolutions algorithm in A^m

INPUT: $M := [\mathbf{f}_1 \;\cdots\; \mathbf{f}_s]^T \in \mathcal{M}_{s\times m}(A)$ with $\mathbf{f}_i \in A^m$, $1 \leq i \leq s$.

OUTPUT: List F of matrices $[F_0, \dots, F_r]$ of Theorem 1.4.29.

INITIALIZATION: List F with $F_0 := M^T$, $i := 0$.

WHILE $Syz(F_i) \neq 0$ **DO**

$F_{i+1} := Syz(F_i)$

$i := i + 1$

RETURN F

The statement that computes a free resolution of a submodule $S := \langle \boldsymbol{f}_1, \dots, \boldsymbol{f}_n \rangle$ of A^m is as follows:

`FreeResolution(`M, ord, ORD, A`)`

Next we will illustrate examples of the implementation of algorithm implemented in Maple.

Example 4.2.5. Considering the extension $A := \sigma(\mathbb{Q})\langle x, y\rangle$, subject to relation: $yx = xy + x$. We will calculate a free resolution for the left module

$S := \langle (1, 1), (xy, 0), (y^2, 0), (0, x)\rangle$.

Using the statement `FreeResolution(`M, gradlex, TOP, A`)` for the matrix

$$M := \begin{bmatrix} 1 & 1 \\ xy & 0 \\ y^2 & 0 \\ 0 & x \end{bmatrix},$$

we get $[F_0, F_1]$, where

$$F_0 = \begin{bmatrix} 1 & xy & y^2 & 0 \\ 1 & 0 & 0 & x \end{bmatrix}, \quad F_1 = \begin{bmatrix} -xy & -xy^2 - 2xy \\ 1 & 2 \\ 0 & x \\ y-1 & y^2-1 \end{bmatrix}, \text{ and } F_r = 0 \text{ for } r > 1.$$

Therefore, a free resolution for S is given by

$$0 \longrightarrow A^2 \xrightarrow{\begin{bmatrix} -xy & -xy^2 - 2xy \\ 1 & 2 \\ 0 & x \\ y-1 & y^2-1 \end{bmatrix}} A^4 \xrightarrow{\begin{bmatrix} 1 & xy & y^2 & 0 \\ 1 & 0 & 0 & x \end{bmatrix}} M \longrightarrow 0.$$

Example 4.2.6. Considering the diffusion algebra $A := \sigma(\mathbb{Q}[x_1, x_2])\langle x, y\rangle$, subject to relation $D_2D_1 = 2D_1D_2 + x_2D_1 - x_1D_2$, we will calculate a free resolution for the left ideal $I := \langle x_1^2x_2D_1^2D_2, x_2^2D_1D_2^2\}$. Using the statement `FreeResolution(`M, gradlex, TOP, A`)` for the matrix

$$M := \begin{bmatrix} x_1^2x_2D_1^2D_2 \\ x_2^2D_1D_2^2 \end{bmatrix}$$

we get $[F_0, F_1]$, where

$$F_0 = \begin{bmatrix} x_1^2x_2D_1^2D_2 & x_2^2D_1D_2^2 \end{bmatrix}, \quad F_1 = \begin{bmatrix} x_2D_1D_2 - 3x_2^2D_1 + x_1x_2^2 \\ -4x_1^2D_1^2 + 4x_1^3D_1 - x_1^4 \end{bmatrix} \text{ and } F_r = 0 \text{ for } r > 1.$$

Therefore, a free resolution for I is given by

$$0 \longrightarrow A \xrightarrow{\begin{bmatrix} x_2D_1D_2 - 3x_2^2D_1 + x_1x_2^2 \\ -4x_1^2D_1^2 + 4x_1^3D_1 - x_1^4 \end{bmatrix}} A^2 \xrightarrow{\begin{bmatrix} x_1^2x_2D_1^2D_2 & x_2^2D_1D_2^2 \end{bmatrix}} M \longrightarrow 0.$$

Example 4.2.7. We consider the Witten's algebra $A := \sigma(\mathbb{Q})\langle x, y, z\rangle$, subject to relations

$$zx = xz - x, \quad zy = z + 2y \quad yx = -xy.$$

We will calculate a free resolution for the left module $S := \langle (1, x+y), (0, z), (y, xz)\rangle$. Using the statement `FreeResolution(`M, gradlexrev, TOP, A`)` for the matrix

$$M := \begin{bmatrix} 1 & x+y \\ 0 & z \\ y & xz \end{bmatrix}$$

we get $[F_0, F_1, F_2]$, where

$$F_0 = \begin{bmatrix} 1 & 0 & y \\ x+y & z & xz \end{bmatrix}, \qquad F_2 = \begin{bmatrix} z-3 \\ -x-y \end{bmatrix},$$

$$F_1 = \begin{bmatrix} xyz + y^2z + xy - 2y^2 & yz^2 - yz - 2y \\ x^2y + x^2z - 2xy^2 - xyz - y^3 - 2x^2 + 5xy & xyz + xz^2 - y^2z - 3xy - 7xz - 3y^2 + 10x \\ -xz - yz + x + 4y & -z^2 + 5z - 4 \end{bmatrix}$$

and $F_r = 0$ for $r > 2$. Thus, a free resolution for S is given by

$$0 \longrightarrow A \xrightarrow{\begin{bmatrix} z-3 \\ -x-y \end{bmatrix}} A^2 \xrightarrow{F_1} A^3 \xrightarrow{\begin{bmatrix} 1 & 0 & y \\ x+y & z & xz \end{bmatrix}} M \longrightarrow 0.$$

Example 4.2.8. In this example we take the multiplicative analogue of the Weyl algebra $A := \sigma(\mathbb{Q})\langle x_1, x_2, x_3\rangle = \mathcal{O}_3(\lambda_{ji})$, with $\lambda_{31} = 2$, $\lambda_{32} = 2$ and $\lambda_{21} = -1$, subject to relations:

$x_3x_1 = 2x_1x_3, \quad x_3x_2 = 2x_2x_3 \quad x_2x_1 = -x_1x_2.$

We calculate a free resolution for the left module

$S := \langle (x_1, x_2+1), (x_3, 0), (1, x_2), (x_2, x_1x_3), (x_3 - 1, 0)\rangle.$

Using the statement `FreeResolution(`M, gradlex, TOP, A`)` for the matrix

$$M := \begin{bmatrix} x_1 & x_2+1 \\ x_3 & 0 \\ 1 & x_2 \\ x_2 & x_1x_3 \\ x_3 - 1 & 0 \end{bmatrix}$$

we get $[F_0, F_1, F_2, F_3]$, where

$$F_0 = \begin{bmatrix} x_1 & x_3 & 1 & x_2 & x_3 - 1 \\ x_2 + 1 & 0 & x_2 & x_1x_3 & 0 \end{bmatrix},$$

$$F_1 = \begin{bmatrix} -2x_2 & 0 & 0 & -2x_1x_3 & 0 & 2x_1x_2x_3 - x_2x_3 \\ \ell_{21} & \ell_{22} & \ell_{23} & \ell_{24} & \ell_{25} & \ell_{26} \\ 2x_2 + 2 & 0 & 0 & 2x_1x_3 & 0 & -2x_1x_2x_3 + x_2x_3 + \frac{1}{2}x_3 \\ 0 & 0 & 0 & 2 & 0 & 2x_2 \\ 2x_1x_2 + 2x_2 + 2 & x_3 & 4x_1x_2x_3 & -4x_1^2x_3 + 2x_2 & 4x_1^2x_2x_3 & -4x_1^2x_2x_3 + 2x_2^2 \end{bmatrix},$$

with $\ell_{21} = -2x_1x_2 - 2x_2 - 2$, $\ell_{22} = -x_3 + 1$, $\ell_{23} = -4x_1x_2x_3 + 4x_1x_2$, $\ell_{24} = 4x_1^2x_3 - 2x_1 - 2x_2$, $\ell_{25} = -4x_1^2x_2x_3 + 4x_1^2x_2$ and $\ell_{26} = 4x_1^2x_2x_3 - 2x_2^2 - x_2 - \frac{1}{2}$.

$$F_2 = \begin{bmatrix} 0 & -\frac{1}{4}x_3 & \frac{1}{4}x_3 & -\frac{1}{4}x_3 & -\frac{1}{4}x_3 & -\frac{1}{2}x_3 & 0 & -\frac{1}{4}x_3 \\ m_{21} & m_{22} & m_{23} & m_{24} & m_{25} & m_{26} & m_{27} & m_{28} \\ -2 & 0 & 0 & x_1 & 0 & 0 & 0 & 0 \\ 0 & -x_2 & x_2 & -x_2 & -x_2 & -2x_2 & 0 & -x_2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & 1 & 1 & 2 & 0 & 1 \end{bmatrix},$$

where $m_{21} = 8x_1x_2$, $m_{22} = -4x_1^2x_2 + 2x_1x_2 + x_2 + \frac{1}{2}$, $m_{23} = -2x_1x_2 - x_2 - \frac{1}{2}$, $m_{24} = -4x_1^2x_2 + 2x_1x_2 + x_2 + \frac{1}{2}$, $m_{25} = 2x_1x_2 + x_2 + \frac{1}{2}$, $m_{26} = 4x_1x_2 + 2x_2 + 1$, $m_{27} == 4x_1^2x_2$ and $m_{28} = 2x_1x_2 + x_2 + \frac{1}{2}$.

$$F_3 = \begin{bmatrix} 0 & 0 & \frac{1}{2}x_1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ -2 & -1 & 0 & 0 & 1 \end{bmatrix},$$

and $F_r = 0$ for $r > 3$. Thus, a free resolution for S is given by

$$0 \longrightarrow A^5 \xrightarrow{\begin{bmatrix} 0 & 0 & \frac{1}{2}x_1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ -2 & -1 & 0 & 0 & 1 \end{bmatrix}} A^8 \xrightarrow{F_2} A^6 \xrightarrow{F_1} A^5 \xrightarrow{\begin{bmatrix} x_1 & x_3 & 1 & x_2 & x_3 - 1 \\ x_2 + 1 & 0 & x_2 & x_1x_3 & 0 \end{bmatrix}} M \longrightarrow 0.$$

4.2.3. Computing the left inverse of a matrix

Corollary 4.2.9. *Let A be a bijective skew PBW extension and $F \in M_{r\times s}(A)$ be a rectangular matrix over A. The algorithm below determines if F is left invertible, and in the positive case, it computes the left inverse of F:*

Algorithm for the left inverse of a matrix

INPUT: A rectangular matrix $F \in M_{r\times s}(A)$

OUTPUT: A matrix $L \in M_{s\times r}(A)$ satisfying $LF = I_s$ if it exists, and 0 in other case

INITIALIZATION:

IF $r \leq s$

RETURN 0

IF $r \geq s$, let $G := \{\boldsymbol{g}_1, \dots, \boldsymbol{g}_t\}$ be a Gröbner basis for the left submodule generated by rows of F and $\{\boldsymbol{e}_i\}_{i=1}^s$ be the canonical basis of A^s. Use the division algorithm to verify if $\boldsymbol{e}_i \in \langle G\rangle$ for each $\leq i \leq s$.

IF there exists some $\boldsymbol{e}_i$ such that $\boldsymbol{e}_i \notin \langle G\rangle$,

RETURN 0

IF $\langle G\rangle = A^s$, let $H \in M_{r\times t}(A)$ with the property $G^T = H^T F$, and consider $K := [k_{ij}] \in M_{t\times s}$, where the k_{ij}'s are such that $\boldsymbol{e}_i = k_{1i}\boldsymbol{g}_1 + k_{2i}\boldsymbol{g}_2 + \cdots + k_{ti}\boldsymbol{g}_t$ for $1 \leq i \leq s$. Thus, $I_s = K^T G^T$

RETURN $L := K^T H^T$

Next we will illustrate with examples the implementation of the algorithm in Maple. The statement that computes a left inverse matrix of a matrix M is as follows:

$$\texttt{LeftInverseMatSkewPoly(}M, \mathrm{ord},\ \mathrm{ORD}, A\texttt{)}.$$

Example 4.2.10. Considering the extension $A := \sigma(\mathbb{K})\langle x, y\rangle$, subject to relation: $yx = -xy + 1$.
Case ($\mathbb{K} := \mathbb{Q}$). Given the matrices

$$M^{(1)} := \begin{bmatrix} 1 & 1 \\ xy & 0 \\ x^2 & 0 \\ 1 & y \end{bmatrix} \text{ and } M^{(2)} := \begin{bmatrix} 1 & 1 \\ xy & 1 \\ y^2 & x \\ x & 2 \\ xy^2 & y \end{bmatrix}.$$

Using the statement `LeftInverseMatSkewPoly(`$M^{(k)}$, gradlex, TOPREV, A`)` for $k = 1, 2$, we get the respective left inverse matrices

$$\texttt{left inverse of } M^{(1)} = \begin{bmatrix} xy^2 - y & y+1 & 0 & -xy+1 \\ -xy^2 + y + 1 & -y-1 & 0 & xy-1 \end{bmatrix},$$

$$\texttt{left inverse of } M^{(2)} = \begin{bmatrix} \frac{1}{4}x^2 + \frac{1}{2}x + \frac{1}{4}y + 1 & -\frac{1}{4}y & -\frac{1}{4}x & -\frac{1}{4}x - \frac{1}{2} & 0 \\ -\frac{1}{4}x^2 - \frac{1}{2}x - \frac{1}{4}y & \frac{1}{4}y & \frac{1}{4}x & \frac{1}{4}x + \frac{1}{2} & 0 \end{bmatrix}.$$

Case ($\mathbb{K} := \mathbb{Z}_2$). Given the matrices

$$M^{(3)} := \begin{bmatrix} x & y & 0 \\ y & y^2 & -x \\ x^2 & -xy & 1 \\ x+y & 1 & -y \end{bmatrix} \text{ and } M^{(4)} := \begin{bmatrix} 1 & x & y \\ x+1 & 0 & 0 \\ -xy & 1 & -y \\ xy^2 & y & 1 \\ y^2 & 1 & x+y \end{bmatrix}.$$

Using the statement `LeftInverseMatSkewPoly(`$M^{(k)}$, gradlex, TOPREV, A`)` for $k = 3, 4$, we get the respectives left inverse matrices

$$\texttt{left inverse of } M^{(3)} = \begin{bmatrix} m_{11}^{(3)} & m_{12}^{(3)} & m_{13}^{(3)} & m_{14}^{(3)} \\ m_{21}^{(3)} & m_{22}^{(3)} & m_{23}^{(3)} & m_{24}^{(3)} \\ m_{31}^{(3)} & m_{32}^{(3)} & m_{33}^{(3)} & m_{34}^{(3)} \end{bmatrix},$$

$$\texttt{left inverse of } M^{(4)} = \begin{bmatrix} m_{11}^{(4)} & m_{12}^{(4)} & m_{13}^{(4)} & m_{14}^{(4)} & m_{15}^{(4)} \\ m_{21}^{(4)} & m_{22}^{(4)} & m_{23}^{(4)} & m_{24}^{(4)} & m_{25}^{(4)} \\ m_{31}^{(4)} & m_{32}^{(4)} & m_{33}^{(4)} & m_{34}^{(4)} & m_{35}^{(4)} \end{bmatrix},$$

where

$$\begin{aligned}
m_{11}^{(3)} &= x^2y^4 + x^3y^2 + xy^4 + x^2y^2 + y^4 + x^3 + y^3 + y, \\
m_{12}^{(3)} &= xy^2 + y^3 + y^2 + x, \\
m_{13}^{(3)} &= xy^4 + x^2y^2 + y^4 + xy^2 + y^3 + x^2 + y^2, \\
m_{14}^{(3)} &= xy^3 + xy^2 + y^3 + y^2, \\
m_{21}^{(3)} &= x^2y^4 + x^3y^2 + x^2y^3 + xy^4 + x^3y + xy^3 + y^4 + xy^2 + x^2 + xy + y^2 + y, \\
m_{22}^{(3)} &= xy^2 + y^3 + xy + 1, \\
m_{23}^{(3)} &= xy^4 + x^2y^2 + xy^3 + y^4 + x^2y + y, \\
m_{24}^{(3)} &= xy^3 + y^3 + y + 1, \\
m_{31}^{(3)} &= x, \\
m_{32}^{(3)} &= 0, \\
m_{33}^{(3)} &= 1, \\
m_{34}^{(3)} &= 0,
\end{aligned}$$

and

$m_{11}^{(4)} = xy^2 + xy + y^2 + y,$
$m_{12}^{(4)} = x^2y^3 + x^2y^2 + xy^2 + y^3 + y,$
$m_{13}^{(4)} = xy^2 + y^2,$
$m_{14}^{(4)} = x^2y + x^2 + y + 1,$
$m_{15}^{(4)} = xy + x + y + 1,$
$m_{21}^{(4)} = xy^2 + xy + x + y,$
$m_{22}^{(4)} = x^2y^3 + x^2y^2 + xy^3 + x^2y + y^3 + xy + y^2 + x + y + 1,$
$m_{23}^{(4)} = xy^2 + x^2 + xy,$
$m_{24}^{(4)} = x^2y + x^2 + xy + 1,$
$m_{25}^{(4)} = x + y,$
$m_{31}^{(4)} = x,$
$m_{32}^{(4)} = x^2y + xy^2 + y^3 + xy + x + y + 1,$
$m_{33}^{(4)} = x^2 + xy + y + 1,$
$m_{34}^{(4)} = 0,$
$m_{35}^{(4)} = xy + y + 1.$

Example 4.2.11. Consider the Ore algebra $\sigma(\mathbb{C})\langle x, y, z\rangle := \mathbb{C}[x, y, z; \sigma]$ of Chapter 2, subjects to relations $xy = yx$, $xz = zy$, $yz = zy$ and $\sigma(z) := \overline{z}$. Given the matrices

$$M^{(1)} := \begin{bmatrix} 1 + x^2z & -ix \\ -ixz & 1 \\ ix^3y & xy \end{bmatrix} \text{ and } M^{(2)} := \begin{bmatrix} i - iy^3 & -ixz + 2y^2 \\ -iy^2 & y + i \\ iy^3 & -iy \end{bmatrix},$$

and using the statement `LeftInverseMatSkewPoly(`$M^{(k)}$`,gradlex,TOP,`A`)` for $k = 1, 2$, we get the left inverse matrices

`left inverse of` $M^{(1)} = \begin{bmatrix} 1 & ix & 0 & 0 \\ i & xz & -x^2z + 1 & 0 \end{bmatrix},$

`left inverse of` $M^{(2)} = \begin{bmatrix} \ell_{11}^{(2)} & \ell_{12}^{(2)} & \ell_{13}^{(2)} \\ \ell_{21}^{(2)} & \ell_{22}^{(2)} & \ell_{23}^{(2)} \end{bmatrix},$

where

$\ell_{11}^{(2)} = -xy^3z - ixy^2z + iy^3 - i,$
$\ell_{12}^{(2)} = ix^2y^2z^2 + 2xy^4z + x^2yz^2 + 3ixy^3z + 2xy^2z - 2iy^4 + y^3 - ixz + 2iy,$
$\ell_{13}^{(2)} = -ix^2yz^2 - 3xy^3z - x^2z^2 - 4ixy^2z - 2xyz + 3iy^3 - xz - y^2 - 2i,$
$\ell_{21}^{(2)} = -y^3 - iy^2,$
$\ell_{22}^{(2)} = ixy^2z + 2y^4 + xyz + 3iy^3 + y^2 - i,$
$\ell_{23}^{(2)} = -ixyz - 3y^3 - xz - 4iy^2 - y - 1.$

Example 4.2.12. Now we take the Witten's algebra $\sigma(\mathbb{Q})\langle x, y, z\rangle$, subjects to relations

$zx = xz - x, \quad zy = yz + 2y,$ and $yx = 2xy$.

Given the matrix

$$M := \begin{bmatrix} x & 2y \\ 1 & -z \\ y & 1 \\ -z & 0 \end{bmatrix}$$

and using the statement `LeftInverseMatSkewPoly(`M`,gradlex,TOP,`A`)`, we get the left inverse matrix of M

$$\begin{bmatrix} -\frac{3}{4}yz + \frac{3}{2}y - z + \frac{5}{4} & -\frac{3}{2}y^2 - \frac{9}{4}x - 2y + 1 & -\frac{9}{4}xz + \frac{3}{2}y + z & -\frac{15}{4}xy - x + y \\ -\frac{3}{8}yz + \frac{3}{4}y - \frac{1}{2}z + \frac{5}{8} & -\frac{3}{4}y^2 - \frac{9}{8}x - y & -\frac{9}{8}xz + \frac{3}{4}y + 1 & -\frac{15}{8}xy - \frac{1}{2}x \end{bmatrix}.$$

Example 4.2.13. Consider the multiplicative analogue of Weyl algebra
$A := \sigma(\mathbb{Q})\langle x_1, x_2, x_3\rangle = \mathcal{O}_2(\lambda_{ji})$, with $\lambda_{31} = 2$, $\lambda_{32} = 2$ and $\lambda_{21} = -1$. Given the matrix

$$M := \begin{bmatrix} x_1x_2 & 1 \\ -x_1x_3 & x_3 + 1 \\ x_2 & x_3 \\ 1 & x_1x_3 \end{bmatrix}$$

and using the statement `LeftInverseMatSkewPoly(`M`,gradlex,TOP,`A`)`, we get the left inverse matrix of M

$$\begin{bmatrix} \frac{4}{11}x_1x_2 - \frac{3}{11}x_1x_3 + \frac{4}{11} & -\frac{4}{11}x_1x_2 - \frac{4}{11} & \frac{4}{11}x_1^2x_2 + \frac{8}{11}x_1^2x_3 - \frac{8}{11}x_1 + \frac{4}{11} & \frac{4}{11}x_1x_2 - \frac{4}{11}x_1x_3 - \frac{4}{11}x_2 + 1 \\ -\frac{4}{11}x_1x_2 + \frac{3}{11}x_1x_3 + \frac{7}{11} & \frac{4}{11}x_1x_2 + \frac{4}{11} & -\frac{4}{11}x_1^2x_2 - \frac{8}{11}x_1^2x_3 - \frac{3}{11}x_1 - \frac{4}{11} & -\frac{4}{11}x_1x_2 + \frac{4}{11}x_1x_3 + \frac{4}{11}x_2 \end{bmatrix}.$$

4.3. Algorithm for the Quillen-Suslin theorem

In this section we present the algorithm for computing the matrix U in the proof of Quillen-Suslin theorem for Ore extensions (Theorem 2.6.1); the algorithm also calculates the basis of a given finitely generated projective module (Theorem 1.1.3). We present two versions of the algorithm, a constructive simplified version and a more complete computational version.

Algorithm for the Quillen-Suslin theorem:
Constructive version

INPUT: An Ore extension $A := K[x, \sigma, \delta]$ (K a field, σ bijective); $F \in M_s(A)$ an idempotent matrix.

OUTPUT: Matrices U, U^{-1} and a basis X of $\langle F \rangle$, where

$$UFU^{-1} = \begin{bmatrix} 0 & 0 \\ 0 & I_r \end{bmatrix} \text{ and } r = dim(\langle F \rangle). \tag{4-5}$$

INITIALIZATION: $F_1 := F$.

FOR k from 1 to $n-1$ **DO**

1. Follow the reduction procedures (B1) and (B2) in the proof of Theorem 2.6.1 in order to compute matrices U'_k, U'^{-1}_k and F_{k+1} such that

$$U'_k F_k U'^{-1}_k = \begin{bmatrix} \alpha_k & 0 \\ 0 & F_{k+1} \end{bmatrix}, \text{ where } \alpha_k \in \{0, 1\}.$$

2. $U_k := \begin{bmatrix} I_{k-1} & 0 \\ 0 & U'_k \end{bmatrix} U_{k-1}$; compute U_k^{-1}.
3. By permutation matrices modify U_{n-1}.

RETURN $U := U_{n-1}$, U^{-1} satisfying (4-5), and a basis X of $\langle F \rangle$.

Example 4.3.1. For $A := K[x, \sigma, \delta]$, with $K := \mathbb{C}$, $\sigma(z) := \overline{z}$ and $\delta := 0$, we consider in $M_4(A)$ the idempotent matrix

$$F = \begin{bmatrix} 1 - ix - x^2 + (1+i)x^3 & -1 + (2-i)x^2 + (-1-i)x^3 & -i - x + (1+i)x^2 & 1 + ix + (-1+i)x^2 \\ -ix + (1+i)x^3 & ix + (1-i)x^2 + (-1-i)x^3 & -i + (1+i)x^2 & 1 + (-1+i)x^2 \\ ix^2 & -x - ix^2 & 1 + ix & x \\ x^3 - x^2 & -ix + (1-i)x^2 - x^3 & x^2 - x & 1 + ix + ix^2 \end{bmatrix}.$$

We apply the constructive version of the Quillen-Suslin algorithm, i.e., following the reductions (B1) and (B2), we compute the matrices U_k and F_k, for $1 \leq k \leq 3$:

$$U_1 = \begin{bmatrix} 1 - ix - x^2 + (1+i)x^3 & -1 + (2-i)x^2 + (-1-i)x^3 & -i - x + (1+i)x^2 & 1 + ix + (-1+i)x^2 \\ x & -i - x & 1 & i \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$U_1^{-1} = \begin{bmatrix} 1 & i+x+(-1-i)x^2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -x & 1+ix-x^2+(1-i)x^3 & i+x & -i \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$U_1FU_1^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -i+(1+i)x^2 & 1 & 0 \\ 0 & x^2-x & 0 & 1 \end{bmatrix}, F_2 = \begin{bmatrix} 0 & 0 & 0 \\ -i+(1+i)x^2 & 1 & 0 \\ x^2-x & 0 & 1 \end{bmatrix};$$

$$U_2 = \begin{bmatrix} 1-ix-x^2+(1+i)x^3 & -1+(2-i)x^2+(-1-i)x^3 & -i-x+(1+i)x^2 & 1+ix+(-1+i)x^2 \\ ix+(-1-i)x^3 & -ix+(-1+i)x^2+(1+i)x^3 & i+(-1-i)x^2 & -1+(1-i)x^2 \\ x & -i-x & 1 & i \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$U_2^{-1} = \begin{bmatrix} 1 & 0 & i+x+(-1-i)x^2 & 0 \\ 0 & -1 & i+(-1-i)x^2 & 0 \\ -x & -i-x & -ix^2 & -i \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$U_2FU_2^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & x^2-x & 1 \end{bmatrix}, F_3 = \begin{bmatrix} 0 & 0 \\ x^2-x & 1 \end{bmatrix};$$

$$U_3 = \begin{bmatrix} 1-ix-x^2+(1+i)x^3 & -1+(2-i)x^2+(-1-i)x^3 & -i-x+(1+i)x^2 & 1+ix+(-1+i)x^2 \\ ix+(-1-i)x^3 & -ix+(-1+i)x^2+(1+i)x^3 & i+(-1-i)x^2 & -1+(1-i)x^2 \\ -x^3+x^2 & ix+(-1+i)x^2+x^3 & -x^2+x & -1-ix-ix^2 \\ x & -i-x & 1 & i \end{bmatrix},$$

$$U_3^{-1} = \begin{bmatrix} 1 & 0 & 0 & i+x+(-1-i)x^2 \\ 0 & -1 & 0 & i+(-1-i)x^2 \\ -x & -i-x & i & -ix \\ 0 & 0 & -1 & -x^2+x \end{bmatrix},$$

$$U_3FU_3^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, F_4 = \begin{bmatrix} 0 \end{bmatrix}.$$

Finally, using permutation matrices, we get

$$U = \begin{bmatrix} x & -i-x & 1 & i \\ 1-ix-x^2+(1+i)x^3 & -1+(2-i)x^2+(-1-i)x^3 & -i-x+(1+i)x^2 & 1+ix+(-1+i)x^2 \\ ix+(-1-i)x^3 & -ix+(-1+i)x^2+(1+i)x^3 & i+(-1-i)x^2 & -1+(1-i)x^2 \\ -x^3+x^2 & ix+(-1+i)x^2+x^3 & -x^2+x & -1-ix-ix^2 \end{bmatrix},$$

$$U^{-1} = \begin{bmatrix} i+x+(-1-i)x^2 & 1 & 0 & 0 \\ i+(-1-i)x^2 & 0 & -1 & 0 \\ -ix & -x & -i-x & i \\ -x^2+x & 0 & 0 & -1 \end{bmatrix},$$

$$UFU^{-1}=\begin{bmatrix}0&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}.$$

So, $r=3$ and the last three rows of U conform a basis $X=\{\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3\}$ of $\langle F\rangle$,

$$\begin{gathered}\boldsymbol{x}_1=(1-ix-x^2+(1+i)x^3,-1+(2-i)x^2+(-1-i)x^3,-i-x+(1+i)x^2,1+ix+(-1+i)x^2),\\ \boldsymbol{x}_2=(ix+(-1-i)x^3,-ix+(-1+i)x^2+(1+i)x^3,i+(-1-i)x^2,-1+(1-i)x^2),\\ \boldsymbol{x}_3=(-x^3+x^2,ix+(-1+i)x^2+x^3,-x^2+x,-1-ix-ix^2).\end{gathered}$$

Next we present a second illustration of the constructive algorithm.

Example 4.3.2. Let $M_4(A)$, where $A:=K[x,\sigma,\delta]$, $K:=\mathbb{Q}(t)$, $\sigma:=id_{\mathbb{Q}(t)}$ and $\delta:=\frac{d}{dt}$; we consider the idempotent matrix $F:=[F^{(1)}\ F^{(2)}\ F^{(3)}\ F^{(4)}]$, $F^{(i)}$ the ith column of F, where

$$F^{(1)}=:\begin{bmatrix}2+2t+(13t^2-5t)x+(8t^3-6t^2)x^2+t^3(t-1)x^3\\2t^2+t+(13t^3-8t^2)x+(8t^4-7t^3)x^2+t^4(t-1)x^3\\3t+2+(14t^2-8t)x+(8t^3-7t^2)x^2+t^3(t-1)x^3\\t^2+t+(t^3+6t^2)x+6t^3x^2+t^4x^3\end{bmatrix},$$

$$F^{(2)}=:\begin{bmatrix}-t^3x^3-5t^2x^2-3tx+1\\t+(-3t^2+2t)x+(-5t^3+t^2)x^2-t^4x^3\\-t^3x^3-5t^2x^2-3tx+1\\-t^3x^3-5t^2x^2-3tx+1\end{bmatrix},$$

$$F^{(3)}=:\begin{bmatrix}t^3x^3+5t^2x^2+3tx-1\\t^4x^3+5t^3x^2+2t^2x-2t\\-t-1+(-t^2+5t)x+6t^2x^2+t^3x^3\\-t^2+t+(-t^3+6t^2)x+2t^3x^2\end{bmatrix},$$

$$F^{(4)}=:\begin{bmatrix}0\\tx\\tx\\1+(t^2-2t)x-t^2x^2\end{bmatrix}.$$

Applying the algorithm we obtain

$$U^{(1)}=:\begin{bmatrix}2t+1+(10t^2-5t)x+(7t^3-6t^2)x^2+(t^4-t^3)x^3\\-3t-2+(-14t^2+8t)x+(-8t^3+7t^2)x^2+(-t^4+t^3)x^3\\-2t+2-t(t-1)x\\-2t^2+7t-2-t(4t^2-21t+10)x-t^2(t^2-10t+7)x^2+t^3(t-1)x^3\end{bmatrix},$$

$$U^{(2)}=:\begin{bmatrix}-t^3x^3-4t^2x^2-tx\\t^3x^3+5t^2x^2+3tx-1\\tx+1\\2t(t-3)x+t^2(t-6)x^2-t^3x^3\end{bmatrix},$$

$$U^{(3)} =: \begin{bmatrix} -t-1+(-t^2+3t)x+5t^2x^2+t^3x^3 \\ t+2+(t^2-5t)x-6t^2x^2-t^3x^3 \\ -tx-1 \\ -t+1-t(2t-7)x-t^2(t-6)x^2+t^3x^3 \end{bmatrix},$$

$$U^{(4)} =: \begin{bmatrix} tx \\ -tx \\ 0 \\ 1 \end{bmatrix};$$

$$(U^{-1})^{(1)} =: \begin{bmatrix} tx+1 \\ t-2+t(t-1)x \\ 0 \\ -t+2-t(t-4)x+t^2x^2 \end{bmatrix},$$

$$(U^{-1})^{(2)} =: \begin{bmatrix} tx+1 \\ t-1+t(t-1)x \\ 1 \\ 1+(-t^2+3t)x+t^2x^2 \end{bmatrix},$$

$$(U^{-1})^{(3)} =: \begin{bmatrix} -t^2x^2-2tx+1 \\ t+(-4t^2+4t)x+(-2t^3+5t^2)x^2+t^3x^3 \\ 1+(-2t^2+t)x+(-t^3+4t^2)x^2+t^3x^3 \\ 1+(-2t^3+8t^2-5t)x+(-t^4+11t^3-18t^2)x^2+(2t^4-9t^3)x^3-t^4x^4 \end{bmatrix},$$

$$(U^{-1})^{(4)} =: \begin{bmatrix} 0 \\ tx \\ tx \\ 1+(t^2-2t)x-t^2x^2 \end{bmatrix}.$$

With these computations we have

$$UFU^{-1} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

thus, $r = 2$ and a base of $\langle F \rangle$ is $X = \{\boldsymbol{x}_1, \boldsymbol{x}_2\}$, with

$$\boldsymbol{x}_1 = (-2t+2-t(t-1)x, tx+1, -tx-1, 0),$$

$$\boldsymbol{x}_2 = (-2t^2+7t-2-t(4t^2-21t+10)x-t^2(t^2-10t+7)x^2+t^3(t-1)x^3, 2t(t-3)x+t^2(t-6)x^2-t^3x^3, -t+1-t(2t-7)x-t^2(t-6)x^2+t^3x^3, 1).$$

Algorithm for the Quillen-Suslin theorem:
Computational version

REQUIRE: $A := K[x;\sigma,\delta]$ and an idempotent matrix $F \in M_s(A)$.

$k := 0$, $F' := F$;
WHILE $k < s-1$ **DO**
  $k := k+1$
  IF $\max\{\deg(f'_{ij}) \mid i = 1 \text{ or } j = 1\} = -\infty$ **THEN**
    $F' := SubMatrix(F', 2..s, 2..s)$;
  ELSE
    (B):
    IF $f'_{11} = 0$ **THEN**
      if $(f'_{1k} \neq 0)$ $F' := T_{k1}(-1)F'T_{k1}(-1)^{-1}$;
      if $(f'_{k1} \neq 0)$ $F' := T_{1k}(-1)F'T_{1k}(-1)^{-1}$;
    END IF
    (B1):
    IF $f'_{11} \in K - \{0\}$ **THEN**
      Apply: OrderReduction1;
    ELSE
      Apply: (B2) OrderReduction2;
    END IF
  END IF
END WHILE
RETURN Matrices U, U^{-1}, UFU^{-1}; a basis X of $\langle F \rangle$; process step by step.

Example 4.3.3. In this example we will illustrate the computational version of the Quillen-Suslin algorithm; let $M_3(A)$, where $A := K[x,\sigma,\delta]$, $K := \mathbb{Q}(t)$, $\sigma(\frac{p(t)}{q(t)}) := \frac{p(t-1)}{q(t-1)}$ and $\delta := 0$; we have the idempotent matrix

$$F = \begin{bmatrix} 1 - \frac{2t}{1+t}x & 2t - \frac{2t(3+2t)}{1+t}x & \frac{2t}{(1+t)^2}x \\ \frac{1}{1+t}x & \frac{3+2t}{1+t}x & \frac{-1}{(1+t)^2}x \\ \frac{t}{1+t}x & -t + \frac{t(3+2t)}{1+t}x & 1 - \frac{t}{(1+t)^2}x \end{bmatrix}.$$

Let $F' := F$, along the example, we will replace the matrices F', U and U^{-1} for the new versions given by the procedures of the algorithm.
Step 1. Since $f'_{11} = 1 - \frac{2t}{1+t}x$, we will apply the reduction procedure of (B2), i.e, OrderReduction2:
Step1.1: The idea is to convert $f'_{1,i} = 0$ for $i > 2$ and $f'_{1,2} \neq 0$.

Applying first $T_{2,3}(\frac{-1}{t(1+2t)})$, then $T_{3,2}(t(1+2t)-\frac{t(3+2t)(1+2t)}{1+t}x)$, and finally permuting the rows and columns 2 and 3, we get

$$UFU^{-1} = \begin{bmatrix} 1-\frac{2t}{1+t}x & \frac{2}{1+2t} & 0 \\ \frac{t(1+2t)}{1+t}x - \frac{2t(1+2t)}{t+2}x^2 & \frac{2t(1+2t)}{(3+2t)(1+t)}x & 0 \\ \frac{2t}{(1+2t)(1+t)}x & \frac{-2}{(1+2t)^2} & 1 \end{bmatrix},$$

where

$$U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & t(1+2t)-\frac{t(3+2t)(1+2t)}{1+t}x & \frac{t(1+2t)}{(1+t)^2}x \\ 0 & 1 & \frac{-1}{t(1+2t)} \end{bmatrix},$$

$$U^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{t(1+2t)} & \frac{3+2t}{1+t}x \\ 0 & 1 & -t(1+2t)+\frac{t(3+2t)(1+2t)}{1+t}x \end{bmatrix}.$$

Step 1.2. Since the new F' is

$$F' = \begin{bmatrix} 1-\frac{2t}{1+t}x & \frac{2}{1+2t} & 0 \\ \frac{t(1+2t)}{1+t}x - \frac{2t(1+2t)}{t+2}x^2 & \frac{2t(1+2t)}{(3+2t)(1+t)} & 0 \\ \frac{2t}{(1+2t)(1+t)}x & \frac{-2}{(1+2t)^2} & 1 \end{bmatrix},$$

we want to reduce the degree of $f'_{1,1}$; for this we apply $T_{2,1}(\frac{-t(1+2t)}{(1+t)}x)$ and we obtain

$$UFU^{-1} = \begin{bmatrix} 1 & \frac{2}{1+2t} & 0 \\ 0 & 0 & 0 \\ 0 & \frac{-2}{(1+2t)^2} & 1 \end{bmatrix},$$

where the new U and U^{-1} are

$$U = \begin{bmatrix} 1 & 0 & 0 \\ \frac{-t(1+2t)}{1+t}x & t(1+2t)-\frac{t(3+2t)(1+2t)}{1+t}x & \frac{t(1+2t)}{(1+t)^2}x \\ 0 & 1 & \frac{-1}{t(1+2t)} \end{bmatrix},$$

$$U^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ \frac{x}{1+t} & \frac{1}{t(1+2t)} & \frac{3+2t}{1+t}x \\ \frac{t(1+2t)}{1+t}x & 1 & -t(1+2t)+\frac{t(3+2t)(1+2t)}{1+t}x \end{bmatrix}.$$

Step 2. The new F' is

$$F' = \begin{bmatrix} 1 & \frac{2}{1+2t} & 0 \\ 0 & 0 & 0 \\ 0 & \frac{-2}{(1+2t)^2} & 1 \end{bmatrix};$$

since $f'_{1,1} = 1$ we apply (B1), i.e., OrderReduction1, for this we consider the matrices

$$S = \begin{bmatrix} 1 & \frac{2}{1+2t} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \text{ and } S^{-1} = \begin{bmatrix} 1 & \frac{-2}{1+2t} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

and then

$$S\,F'S^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & \frac{-2}{(1+2t)^2} & 1 \end{bmatrix}.$$

Therefore, the new F' is

$$F' = \begin{bmatrix} 0 & 0 \\ \frac{-2}{(1+2t)^2} & 1 \end{bmatrix}, \text{ and } UFU^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & \frac{-2}{(1+2t)^2} & 1 \end{bmatrix},$$

where the new U and U^{-1} are

$$U = \begin{bmatrix} 1 - \frac{2t}{1+t}x & 2t - \frac{2t(3+2t)}{1+t}x & \frac{2t}{(1+t)^2}x \\ \frac{-t(1+2t)}{1+t}x & t(1+2t) - \frac{t(3+2t)(1+2t)}{1+t}x & \frac{t(1+2t)}{(1+t)^2}x \\ 0 & 1 & \frac{-1}{t(1+2t)} \end{bmatrix},$$

$$U^{-1} = \begin{bmatrix} 1 & \frac{-2}{1+2t} & 0 \\ \frac{x}{1+t} & \frac{1}{t(1+2t)} - \frac{2}{(1+t)(3+2t)}x & \frac{3+2t}{1+t}x \\ \frac{t(1+2t)}{1+t}x & 1 - \frac{2t(1+2t)}{(1+t)(3+2t)}x & -t(1+2t) + \frac{t(3+2t)(1+2t)}{1+t}x \end{bmatrix}.$$

Since $f'_{1,1} = 0$, we apply $T_{1,2}(-1)$, we get

$$UFU^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{2}{(1+2t)^2} & \frac{-4t^2-4t+1}{(1+2t)^2} \\ 0 & \frac{-2}{(1+2t)^2} & \frac{4t^2+4t-1}{(1+2t)^2} \end{bmatrix} \text{ and } F' = \begin{bmatrix} \frac{2}{(1+2t)^2} & \frac{-4t^2-4t+1}{(1+2t)^2} \\ \frac{-2}{(1+2t)^2} & \frac{4t^2+4t-1}{(1+2t)^2} \end{bmatrix},$$

where the new U and U^{-1} are

$$U = \begin{bmatrix} 1 - \frac{2t}{1+t}x & 2t - \frac{2t(3+2t)}{1+t}x & \frac{2t}{(1+t)^2}x \\ \frac{-t(1+2t)}{1+t}x & 2t^2 + t - 1 - \frac{t(3+2t)(1+2t)}{1+t}x & \frac{1}{t(1+2t)} + \frac{t(1+2t)}{(1+t)^2}x \\ 0 & 1 & \frac{-1}{t(1+2t)} \end{bmatrix},$$

$$U^{-1} = \begin{bmatrix} 1 & \frac{-2}{1+2t} & \frac{-2}{1+2t} \\ \frac{1}{1+t}x & \frac{1}{t(1+2t)} - \frac{2}{(1+t)(3+2t)}x & \frac{1}{t(1+2t)} + \frac{4t^2+12t+7}{(1+t)(3+2t)}x \\ \frac{t(1+2t)}{1+t}x & 1 - \frac{2t(1+2t)}{(1+t)(3+2t)}x & -2t^2 - t + 1 + \frac{t(1+2t)(4t^2+12t+7)}{(1+t)(3+2t)}x \end{bmatrix}.$$

Since $f'_{1,1} = \frac{2}{(1+2t)^2}$ is invertible, we apply OrderReduction1 with matrices

$$T = \begin{bmatrix} 1 & -2t^2 - 2t + \frac{1}{2} \\ 1 & 1 \end{bmatrix} \text{ and } T^{-1} = \begin{bmatrix} \frac{2}{(1+2t)^2} & \frac{4t^2+4t-1}{(1+2t)^2} \\ \frac{-2}{(1+2t)^2} & \frac{2}{(1+2t)^2} \end{bmatrix},$$

so

$$T\,F'T^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Thus, the new F' is

$$F' = \begin{bmatrix} 0 \end{bmatrix} \text{ and } UFU^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

where the new U and U^{-1} are

$$U = \begin{bmatrix} 1 - \frac{2t}{1+t}x & 2t - \frac{2t(3+2t)}{1+t}x & \frac{2t}{(1+t)^2}x \\ \frac{-t(1+2t)}{1+t}x & -t - \frac{1}{2} - \frac{t(3+2t)(1+2t)}{1+t}x & \frac{1+2t}{2t} + \frac{t(1+2t)}{(1+t)^2}x \\ \frac{-t(1+2t)}{1+t}x & 2t^2 + t - \frac{t(3+2t)(1+2t)}{1+t}x & \frac{t(1+2t)}{(1+t)^2}x \end{bmatrix},$$

$$U^{-1} = \begin{bmatrix} 1 & 0 & \frac{-2}{1+2t} \\ \frac{x}{1+t} & \frac{-2}{(1+t)(3+2t)}x & \frac{1}{t(1+2t)} \\ \frac{t(1+2t)}{1+t}x & \frac{2t}{1+2t} - \frac{2t(1+2t)}{(1+t)(3+2t)}x & \frac{1}{1+2t} \end{bmatrix}.$$

Permuting, we have finally

$$UFU^{-1} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

where the new U and U^{-1} are

$$U = \begin{bmatrix} \frac{-t(1+2t)}{1+t}x & 2t^2 + t - \frac{t(3+2t)(1+2t)}{1+t}x & \frac{t(1+2t)}{(1+t)^2}x \\ 1 - \frac{2t}{1+t}x & 2t - \frac{2t(3+2t)}{1+t}x & \frac{2t}{(1+t)^2}x \\ \frac{-t(1+2t)}{1+t}x & -t - \frac{1}{2} - \frac{t(3+2t)(1+2t)}{1+t}x & \frac{1+2t}{2t} + \frac{t(1+2t)}{(1+t)^2}x \end{bmatrix},$$

$$U^{-1} = \begin{bmatrix} \frac{-2}{1+2t} & 1 & 0 \\ \frac{1}{t(1+2t)} & \frac{1}{1+t}x & \frac{-2}{(1+t)(3+2t)}x \\ \frac{1}{1+2t} & \frac{t(1+2t)}{1+t}x & \frac{2t}{1+2t} - \frac{2t(1+2t)}{(1+t)(3+2t)}x \end{bmatrix}.$$

Therefore, $r = 2$ and the last two rows of U conform a basis $X = \{\boldsymbol{x}_1, \boldsymbol{x}_2\}$, of $\langle F \rangle$,

$$\boldsymbol{x}_1 = (1 - \tfrac{2t}{1+t}x, 2t - \tfrac{2t(3+2t)}{1+t}x, \tfrac{2t}{(1+t)^2}x),\ \boldsymbol{x}_2 = (\tfrac{-t(1+2t)}{1+t}x, -t - \tfrac{1}{2} - \tfrac{t(3+2t)(1+2t)}{1+t}x, \tfrac{1+2t}{2t} + \tfrac{t(1+2t)}{(1+t)^2}x).$$

Example 4.3.4. Let $M_4(A)$, where $A := K[x, \sigma, \delta]$, $K := \mathbb{Q}(t)$, $\sigma(f(t)) := f(qt)$ and $\delta(f(t)) = \frac{f(qt)-f(t)}{t(q-1)}$ where $q \in K - 0$; we consider the idempotent matrix F given by

$F := [F^{(1)}\ F^{(2)}\ F^{(3)}\ F^{(4)}]$, $F^{(i)}$ the ith column of F and $a \in \mathbb{Q}$, where

$$F^{(1)} = \begin{bmatrix} -t^2qx^2 \\ (-ta+2\,t)\,x-2\,a+2 \\ tx+2 \\ -1 \end{bmatrix},$$

$$F^{(2)} = \begin{bmatrix} -2\,tx+2 \\ -t^2qx^2+(ta-4\,t)\,x+2\,a-1 \\ -tx-2 \\ tx+2 \end{bmatrix},$$

$$F^{(3)} = \begin{bmatrix} -tx-2 \\ (-2\,t^2qa+3\,t^2q)\,x^2+(a^2t-8\,ta+8\,t)\,x+2\,a^2-3\,a+1 \\ t^2qx^2+(-ta+4\,t)\,x-2\,a+2 \\ (ta-2\,t)\,x+2\,a-2 \end{bmatrix},$$

$$F^{(4)} = \begin{bmatrix} -t^3q^3x^3+(-q^2t^2-5\,t^2q)\,x^2-5\,tx+2 \\ -t^3q^3x^3+(-q^2t^2-3\,t^2q)\,x^2+(-ta+t)\,x-2\,a+2 \\ tx+2 \\ t^2qx^2+2\,tx-1 \end{bmatrix}.$$

Applying the algorithm we obtain

$$U = \begin{bmatrix} tx+1 & 0 & t^2qx^2+2\,tx-1 & t^2qx^2+3\,tx \\ 1 & -tx-2 & (-ta+2\,t)\,x-2\,a+2 & -t^2qx^2-2\,tx+2 \\ tx-1 & 1 & t^2qx^2+a-1 & t^2qx^2+2\,tx-1 \\ 1 & 0 & tx & tx+1 \end{bmatrix},$$

$$U^{-1} = \begin{bmatrix} tx & -1 & -tx-2 & 0 \\ a-1 & -tx+a-1 & -t^2qx^2+(ta-4\,t)\,x+2\,a-1 & t^3q^3x^3-(-q+a-4)\,t^2qx^2+(-3\,ta+3\,t)\,x+1 \\ -1 & -1 & -tx-2 & t^2qx^2+3\,tx \\ 0 & 1 & tx+2 & -t^2qx^2-2\,tx+1 \end{bmatrix},$$

$$UFU^{-1} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

Therefore, $r=2$ and the last two rows of U conform a basis $X=\{\boldsymbol{x}_1,\boldsymbol{x}_2\}$, of $\langle F\rangle$,

$$\boldsymbol{x}_1 = (tx-1, 1, t^2qx^2+a-1, t^2qx^2+2\,tx-1),\ \boldsymbol{x}_2 = (1,0,tx,tx+1).$$

Next we present some comments about the implementation of the computational version of the Quillen-Suslin algorithm.

Remark 4.3.5. The OrderReduction1 is based in the implementation of the procedure $(B1)$ in the proof of Theorem 2.6.1; for the OrderReduction2, the following algorithm describes its functionality:

Algorithm OrderReduction2

REQUIRE: $A := K[x;\sigma,\delta]$ and an idempotent matrix $F \in M_s(A)$ with $\deg(f_{11}) \geq 1$.

1: Make $f_{1,j} = 0$ for $j > 2$ and $f_{1,2} \neq 0$;
2: Reduce degree of $f_{1,1}$;
3: **IF** $f_{1,1} = 0$
4: **IF** $\max\{\deg(f_{i,j}) > 0 \mid i = 1 \text{ or } j = 1\} > 0$
5: Make $f_{1,j} = 0$ for $j > 2$ and $f_{1,2} \neq 0$;
6: $F := P_{12}\, F\, P_{12}$;
7: Apply: OrderReduction1;
8: **ELSE**
9: $F' := SubMatrix(F, 2..s, 2..s)$;
10: **ENDIF**
11: **ELSE**
12: Apply: OrderReduction1;
13: **ENDIF**
14: **RETURN** Matrices U, U^{-1}, F' and $UFU^{-1} = \begin{bmatrix} \alpha & 0 \\ 0 & F' \end{bmatrix}$, with $\alpha \in \{0,1\}$.

Remark 4.3.6. For the implementation of the Quillen-Suslin algorithm we used Maple® 2016, and we create a library called `OrePolyToolKit.lib` consisting in two packages:

- `OrePolyUtility`: this is a new useful collection of functions for operating matrices, vectors and lists over an `UnivariateOreRing` $K[x;\sigma,\delta]$; the `UnivariateOreRing` structure was taken from the library `OreTools` within the standard Maple libraries.

- `OrePolyQS`: This is the most important new collection of functions related to the Quillen-Suslin algorithm over $K[x;\sigma,\delta]$; the main routine of the algorithm was implemented here, the following functions of this package are fundamentals:
  - `GenerateIdemp`: this function generates idempotent matrices over $K[x;\sigma,\delta]$, the arguments are the matrix order and the `UnivariateOreRing`, and return an idempotent matrix of the given dimension over the respective `UnivariateOreRing`.
  - `QSAlgKsd`: this is the main function of the algorithm, it shows the sequence of all steps of the Quillen-Suslin algorithm presented in this paper; the arguments are the idempotent matrix and the `UnivariateOreRing`, and return the matrix UFU^{-1} in the form of Theorem 2.6.1, the matrices U and U^{-1}, the basis of $\langle F\rangle$ and the complete process step by step.

4.4. Algorithm for computing the generating idempotent in multidimensional convolutional codes

Considering the notation of chapter 3, let A is a finite dimensional semisimple algebra over a finite field $\mathbb{F}$ and let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ and consider $R := A[x_1, \dots, x_n; \sigma]$. Assume that $S := F[x_1, \dots, x_n] \subseteq A[x_1, \dots, x_n; \sigma]$ is a separable ring extension.

Computation of the generating idempotent

INPUT: $L := \{g_0, \dots, g_{t-1}\} \subseteq R$ with $g_i \neq 0$, a separability element $p := \sum_i a_i \otimes b_i$ for the separable ring extension $S \subseteq R$.

OUTPUT: An idempotent $e \in R$ such that $Re = Rg_0 + \cdots Rg_{t-1}$, or zero if it does not exist.

Compute matrices $M(G)$ and H.

IF H is not basic

RETURN 0

ENDIF

Compute matrices P and Q.

$V := [I_{m-k}\ 0]$ where $m = \dim_{\mathbb{F}}(A)$.

$M_h := VP$, $M_s := P^{-1}V^T$, $M := M_s M_h$.

Compute $f_i := \alpha(M \cdot \gamma(b_i))$.

$f := \sum_i a_i f_i$.

RETURN $1 - f$.

Example 4.4.1. Let $\mathbb{F} = \mathbb{F}_4 = F_2(\varepsilon)$ and $A = \mathbb{F}[x]/(x^5 - 1)$. Hence, since $x^5 - 1$ is decomposed as $(x+1) \cdot (x^2 + x + 1) \cdot (x^2 + \varepsilon^2 x + 1)$ in $\mathbb{F}[x]$, $A = K_0 \times K_1 \times K_2$, where

$$K_0 = \frac{\mathbb{F}[x]}{(x+1)},\ K_1 = \frac{\mathbb{F}[x]}{(x^2+x+1)},\ K_2 = \frac{\mathbb{F}[x]}{(x^2+\varepsilon^2 x+1)}.$$

Consider the automorphism $\sigma : A \longrightarrow A$ defined by $\sigma(x) = x^4 + \varepsilon^2 x^3 + \varepsilon x^2 + x$, in order now we must to calculate a separability element $\overline{p}$ of the extension $\mathbb{F}_4[y, z] \subseteq A[y, z; \sigma]$ following the Equation (3-4).

$\{1\}$ is a self-dual normal basis of K_0, $\{x, x^4\}$ and $\{\varepsilon x, (\varepsilon x)^4\}$ are normal dual bases for K_1 and $\{\varepsilon^2 x + 1, (\varepsilon^2 x + 1)^4\}$ and $\{x + \varepsilon, (x + \varepsilon)^4\}$ are normal dual bases for K_2.

We get a separability element

$$\begin{aligned}\overline{p} =&(x^4 + x^3 + x^2 + x + 1) \otimes_{\mathbb{F}_4[y,z]} (x^4 + x^3 + x^2 + x + 1)\\ &+ (\varepsilon^2 x^4 + \varepsilon^2 x^3 + \varepsilon x^2 + \varepsilon) \otimes_{\mathbb{F}_4[y,z]} (x^4 + x^3 + \varepsilon^2 x^2 + \varepsilon^2)\\ &+ (\varepsilon x^3 + \varepsilon^2 x^2 + \varepsilon^2 x + \varepsilon) \otimes_{\mathbb{F}_4[y,z]} (\varepsilon^2 x^3 + x^2 + x + \varepsilon^2)\\ &+ (\varepsilon^2 x^4 + \varepsilon^2 x^2 + \varepsilon x + \varepsilon) \otimes_{\mathbb{F}_4[y,z]} (x^4 + x^2 + \varepsilon^2 x + \varepsilon^2)\\ &+ (\varepsilon x^4 + \varepsilon^2 x^3 + \varepsilon^2 x + \varepsilon) \otimes_{\mathbb{F}_4[y,z]} (\varepsilon^2 x^4 + x^3 + x + \varepsilon^2)\end{aligned}$$

Let I be the left ideal generated by the Ore polynomial in $A[y, z; \sigma]$

$$g = (\varepsilon^2 x^4 + \varepsilon x^3 + \varepsilon x^2 + \varepsilon^2 x)yz^2 + (x^4 + x^3 + x^2 + x)yz + (\varepsilon^2 x^4 + \varepsilon x^3 + \varepsilon x^2 + \varepsilon^2 x + 1).$$

Therefore the matrix $M(g)$ is given by

$$\begin{bmatrix} 1 & \varepsilon^2 yz^2 + yz + \varepsilon^2 & \varepsilon yz^2 + yz + \varepsilon & \varepsilon yz^2 + yz + \varepsilon & \varepsilon^2 yz^2 + yz + \varepsilon^2 \\ \varepsilon^2 yz^2 + yz + \varepsilon^2 & 1 & \varepsilon^2 yz^2 + \varepsilon^2 z + \varepsilon^2 & \varepsilon yz^2 + \varepsilon yz + \varepsilon & \varepsilon yz^2 + \varepsilon \\ \varepsilon yz^2 + yz + \varepsilon & \varepsilon^2 yz^2 + \varepsilon^2 z + \varepsilon^2 & 1 & \varepsilon^2 yz^2 + \varepsilon^2 & \varepsilon yz^2 + \varepsilon yz + \varepsilon \\ \varepsilon yz^2 + yz + \varepsilon & \varepsilon yz^2 + \varepsilon yz + \varepsilon & \varepsilon^2 yz^2 + \varepsilon^2 & 1 & \varepsilon^2 yz^2 + \varepsilon^2 z + \varepsilon^2 \\ \varepsilon^2 yz^2 + yz + \varepsilon^2 & \varepsilon yz^2 + \varepsilon & \varepsilon yz^2 + \varepsilon yz + \varepsilon & \varepsilon^2 yz^2 + \varepsilon^2 z + \varepsilon^2 & 1 \end{bmatrix}$$

Computing matrices P and Q such that $PM(G)Q$ is a basic matrix then we can finish the algorithm and find the idempotent f that generate the ideal.

A. Maple library Documentation

In this appendix we will show the content of the fundamentals packages: SPBWETools, RingTools and SPBWEGrobner, contained in the library SPBWE.lib.

A.1. The package SPBWETools

The package SPBWETools is a collection of functions that allows to define and make computations with skew PBW extensions; to invoke this package we use the follow sentence at the beginning of a Maple spreadsheet.

with(SPBWETools);

In the definition of a skew PBW extension is also important to invoke the package RingTools in order to define the coefficient ring, for this we use the sentence

with(RingTools);

Now, we will define a coefficients ring.

Calling Sequence

`SetCoeffsRing`(Name=*name*, StructRing=*strRing*, charact=*chr*)

Parameters

name: this parameter is a string that define the name coefficient ring, if it is omitted, then *name* is assigned by a default name string.

strRing: this parameter indicates which is the structure of the ring. In this implementation only we have worked with structures of commutative multivariate polynomial rings or subrings predefined in Maple, but is feasible to define new structures of coefficient rings or to use another packages that defines the structure of rings such like UnivariateOreRings or Skew_Algebras; this parameter is *optional*, if it is omitted then the structure is defined as standar, i.e., this is defined as some subring of the fraction ring $K(t_1, \dots, t_m)$, where K is some subring of $\mathbb{C}$ or the ring $\mathbb{Z}_{chr}$.

chr: characteristic of a ring; this parameter is *optional*, if it is omitted then the characteristic assigned is zero.

A.1.1. Skew PBW extensions

Recall Definition 1.3.1 and Proposition 1.3.4. A skew PBW extension $\sigma(R)\langle x_1, \dots, x_n\rangle$ is subject to relations:

$$\begin{aligned} &x_jx_i = c_{ij}x_ix_j + d_1^{(ij)}x_1 + \cdots + d_n^{(ij)}x_n + d_{ij} \quad \text{for } 1 < i < j < n, \\ &x_ir = \sigma_i(r) + \delta_i(r) \quad \text{for } 1 < i < n \text{ with } r \in R. \end{aligned} \tag{A-1}$$

The following parametric description was based in [1], this allows to define a skew PBW extension.

Calling Sequence

`SetSkewPBWExtension`(vars, rels, sigmas, deltas, `R`, *value*)

Parameters

vars: list of variables $[x_1, \dots, x_n]$, this list determines the order $x_1 \succ \dots \succ x_n$.

rels: list of relations $[rel_1, \dots, rel_t]$ determined by (A-1), where each relation rel_k has the form $[[x_i, x_j], c_{ij}, d_1^{(ij)}, \dots, d_n^{(ij)}, d_{ij}]$ for each $i < j$.

`R`: is the coefficient ring `coeffsRing` defined as before for the skew PBW extensions.

sigmas: list of functions $[\sigma_1, \dots, \sigma_n]$ of (A-1).

deltas: list of functions $[\delta_1, \dots, \delta_n]$ of (A-1).

value: boolean parameter that declare the structure

- if *value* is *true* then from [1], the implementation checks if the structure effectively defines a skew PBW extension; in negative case, return "*Non definite Skew PBW extension*", and the structure is not defined; in affirmative case, the implementation return "*This structure represents a Skew PBW Extension*" and the skew PBW extension is defined effectively.
- if *value* is *false* the implementation allows to realize computations with this structure, but this is not defined as skew PBW extension.

This parameter is *optional*, if it is omitted then *value* is predefined as *true*.

Remark

- The correct definition of the skew PBW extension is subject to that each σ_i and δ_i to be effectively injective endomorphism of R and σ_i-derivation, respectively.
- The statement `SetSkewPBWExtension` returns a *type* in Maple called `SPBWE`.

A.1.2. Some useful functions with skew PBW extensions

If a skew PBW extension is effectively defined (or even if the argument *value* is entered as *false*), it is possible to make computations with diverse functions implemented in Maple. Next, we will see these.
We remark that all operations with polynomials in a skew PBW extension are assumed with the order declared in $vars$.

`SkewProd`

This function return the product $p \cdot q$ or the product $\prod_{i=1}^{n} p_i$, where p, q, p_i are polynomials in a skew PBW extension A.

Calling Sequence

`SkewProd`(p, q, A)

`SkewProd`(L, A)

Parameters

p : polynomial in A.

q : polynomial in A.

L : list of polynomials $[p_1, \dots, p_n]$, with $n \geq 2$ in A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`SkewSum`

This function return the sum of two polynomials in a skew PBW extension A.

Calling Sequence

`SkewSum`(p, q, A)

`SkewSum`(L, A)

Parameters

p : polynomial in A.

q : polynomial in A.

L : list of polynomials $[p_1, \dots, p_n]$, with $n \geq 2$ in A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`SkewSubs`

This function returns the substraction $p-q$, where p and q are polynomials in a skew PBW extension A.

Calling Sequence

`SkewSubs`(p, q, A)

Parameters

p : polynomial in A.

q : polynomial in A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`SkewRelation`

This function prints the relation endowed for two variables in a skew PBW extension A.

Calling Sequence

`SkewRelation`(x_i, x_j, A)

Parameters

x_i : variable of a A.

x_j : variable of a A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`deg`

This function returns the degree of a polynomial p in a skew PBW extension A.

Calling Sequence

`deg`(p, A)

Parameters

p : polynomial in A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

CanonicalVector

This function returns the n-dimensional vector $\boldsymbol{e}_i$.

Calling Sequence

`CanonicalVector`(i, n)

Parameters

i : positive integer that indicates the i-th canonical vector.

n : positive integer that indicates the size of the vector.

SkewScalarProd

This function returns the product of a polynomial p by a polynomial vector $\boldsymbol{v}$ over a skew PBW extension A.

Calling Sequence

`SkewScalarProd`$(p, \boldsymbol{v}, A)$

Parameters

p : polynomial in A.

$\boldsymbol{v}$: polynomial vector in A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

SkewPointedProd

This function returns the escalar product $\boldsymbol{u} \cdot \boldsymbol{v}$, where $\boldsymbol{u}$ and $\boldsymbol{v}$ are polynomial vectors over a skew PBW extension A.

Calling Sequence

`SkewScalarProd`$(\boldsymbol{u}, \boldsymbol{v}, A)$

Parameters

$\boldsymbol{u}$: polynomial vector in A.

$\boldsymbol{v}$: polynomial vector in A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`SkewSumVector`

This function returns the sum of two polynomial vectors over a skew PBW extension A.

Calling Sequence

`SkewScalarProd`$(\boldsymbol{u}, \boldsymbol{v}, A)$

Parameters

$\boldsymbol{u}$: polynomial vector over A.

$\boldsymbol{v}$: polynomial vector over A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`SkewMinusVector`

This function returns the vector $-\boldsymbol{v}$ over a skew PBW extension A.

Calling Sequence

`SkewMinusVector`$(\boldsymbol{v})$

Parameters

$\boldsymbol{v}$: polynomial vector over A.

`GeneratePolyMatrix`

This function returns a random matrix with polynomials of degree deg and whose coefficients are integers module mod when mod is positive integer or numbers in $\mathbb{C}$ when mod is zero.

Calling Sequence

`GeneratePolyMatrix`$(rows, cols, vars, \{mod = m\}, \{deg = d\})$

Parameters

$rows$: positive integer that indicates the number of rows of the matrix.

$cols$: positive integer for the number of columns of the matrix.

vars: list of variables $[x_1, \ldots, x_n]$ of polynomials in the matrix.

m : non negative integer that indicates the integer mod, this parameter is optional if is omitted then is assumed by 0.

d : non negative integer for the maximum degree of polynomials in the matrix, this parameter is optional if is omitted then is assumed by 1.

`SkewProdMatrix`

This function returns the matrix product $P \cdot Q$ where P and Q are polynomial matrices over a skew PBW extension A.

Calling Sequence

`SkewProdMatrix`(P, Q, A)

Parameters

P : polynomial matrix over A.

Q : polynomial matrix over A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`SkewSumMatrix`

This function returns the matrix sum of two matrices P and Q over a skew PBW extension A.

Calling Sequence

`SkewSumMatrix`(P, Q, A)

Parameters

P : polynomial matrix over A.

Q : polynomial matrix over A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`SkewSubsMatrix`

This function returns the matrix substraction $P - Q$, where P and Q are polynomial matrices over a skew PBW extension A.

Calling Sequence

`SkewSubsMatrix`(P, Q, A)

Parameters

P : polynomial matrix over A.

Q : polynomial matrix over A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

A.2. The package SPBWEGrobner

The following functions include the main applications of this implementation: the division algorithm, the Buchberger algorithm, the computations of syzygies, free resolutions and the left inverse of a matrix.

lcVector

This function returns the leading coefficient of a polynomial vector over a skew PBW extension A.

Calling Sequence

`lcVector`$(\boldsymbol{v}, ordPoly, ord, A)$

Parameters

$\boldsymbol{v}$: polynomial vector over A.

$ordPoly$: polynomial order over A.

ord : polynomial vector order over A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

ltVector

This function returns the leading term of a polynomial vector over a skew PBW extension A.

Calling Sequence

`ltVector`$(\boldsymbol{v}, ordPoly, ord, A)$

Parameters

$\boldsymbol{v}$: polynomial vector over A.

$ordPoly$: polynomial order over A.

ord : polynomial vector order over A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`lmVector`

This function returns the leading monomial of a polynomial vector over a skew PBW extension A.

Calling Sequence

`lmVector`$(\boldsymbol{v}, ordPoly, ord, A)$

Parameters

$\boldsymbol{v}$: polynomial vector over A.

$ordPoly$: polynomial order over A.

ord : polynomial vector order over A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`PrintSkewPolyVector`

This function print an ordered polynomial vector over a skew PBW extension A according to a polynomial order and vector order.

Calling Sequence

`PrintSkewPolyVector`$(\boldsymbol{v}, vars, ordPoly, ord, R)$

Parameters

$\boldsymbol{v}$: polynomial vector in A.

$vars$: list of variables $[x_1, \ldots, x_n]$, this list determines the order $x_1 \succ \ldots \succ x_n$.

$ordPoly$: polynomial order over A.

ord : polynomial vector order over A.

R : the coefficient ring of the polynomial vector $\boldsymbol{v}$; `coeffsRing` defined as before for the skew PBW extensions.

`DivisionAlgorithm`

According to Subsections 4.1.2 and 4.1.4, this function implements the division algorithm for a skew PBW extension A and returns a list $[Q, h]$, where Q is a list of polynomials (vectors) and h is a polynomial (polynomial vector), satisfying the conditions of division algorithm for ideals (modules).

Calling Sequence

`DivisionAlgorithm`$(f, L, ordPoly, A)$ %% version for ideals

`DivisionAlgorithm`$(\boldsymbol{f}, F, ordPoly, ord, A)$ %% version for modules

Parameters

f : polynomial in A.

L : list $[f_1, \ldots, f_n]$ of polynomials in A.

F : list of polynomial vectors $[\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n]$ over A.

$\boldsymbol{f}$: polynomial vector over A.

$ordPoly$: polynomial order over A.

ord : polynomial vector order over A.

A : skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`BuchbergerAlgSkewPoly`

According the Theorems 4.1.11 and 4.1.20, this function implements the Buchberger's algorithm for a bijective skew PBW extension A and returns a set of polynomial vectors that form a Gröbner basis of a ideal or module.

Calling Sequence

`BuchbergerAlgSkewPoly`$(L, ordPoly, A)$ %% version for ideals

`BuchbergerAlgSkewPoly`$(F, ordPoly, ord, A)$ %% version for modules

Parameters

L : list $[f_1, \ldots, f_n]$ of polynomials in A; the ideal is $\langle f_1, \ldots, f_n\}$.

F : list of polynomial vectors $[\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n]$ over a skew PBW extension A; the module is generated by $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n$.

$ordPoly$: polynomial order over A.

ord : polynomial vector order over A.

A : bijective skew PBW extension, this is a type `SPBWE` defined in A.1.1.

SyzModule

This function calculates the syzygy module of a finite set of polynomial vectors F over a bijective skew PBW extension A. This function returns a matrix whose rows conform the Syzygy module of F.

Calling Sequence

`SyzModule`($M, ordPoly, ord, A$,`view`)

Parameters

M : polynomial matrix over A where each row of M corresponds to a vector of F.

$ordPoly$: polynomial order over A.

ord : polynomial vector order over A.

A : bijective skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`view` : boolean value; when it is *true*, then the function prints preliminary results, and if it is *false*, then the preliminaries are not written; this parameter is optional, if it is omitted, then it is assumed *false*.

FreeResolution

This function calculates a free resolution of left A-module, where A is a bijective skew PBW extension. According to Theorem 1.4.29, this function returns the list of matrices $F = [F_0, F_1, \ldots, F_r]$.

Calling Sequence

`FreeResolution`($M, ordPoly, ord, A$,`view`)

Parameters

M : polynomial matrix over A, this matrix corresponds to F_0 in Theorem 1.4.29.

$ordPoly$: polynomial order over A.

ord : polynomial vector order over A.

A : bijective skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`view` : boolean value; when it is *true*, then the function prints preliminary results, and if it is *false*, then the preliminaries are not written; this parameter is optional, if it is omitted, then it is assumed *false*.

`HQMatrices`

This function computes a list $[H, Q]$, where H and Q are the matrices in Theorem 1.4.8; F is a set of polynomial vectors over a bijective skew PBW extension A.

Calling Sequence

`HQMatrices`$(M, ordPoly, ord, A)$

Parameters

M : polynomial matrix over A whose rows are the vectors of F.

$ordPoly$: polynomial order over A.

ord : polynomial vector order over A.

A : bijective skew PBW extension, this is a type `SPBWE` defined in A.1.1.

`LeftInverseMatrix`

According the Corollary 4.2.9, this function calculates a left inverse of a matrix (if it exists) with entries in a bijective skew PBW extension A.

Calling Sequence

`LeftInverseMatrix`$(M, ordPoly, ord, A)$

Parameters

M : polynomial matrix over A.

$ordPoly$: polynomial order over A.

ord : polynomial vector order over A.

A : bijective skew PBW extension, this is a type `SPBWE` defined in A.1.1.

B. Glossary of skew PBW extensions

The following concrete examples of skew PBW extensions are predefined in the library `SPBWE.lib`.

B.1. PBW extensions

PBW extensions were defined by Bell and Goodearl in 1988 in [15]. PBW extensions are a subclass of the bijective skew PBW extensions $\sigma(R)\langle x_1, \dots, x_n\rangle$, in this case $\sigma_i = i_R$ and $\delta_i = 0$ for each $1 \leq i \leq n$ and $c_{i,j} = 1$ for every $1 \leq i, j \leq n$. A PBW extension is subject to relations:

$$x_j x_i = x_i x_j + d_1^{(ij)} x_1 + \cdots + d_n^{(ij)} x_n + d_{ij} \text{ for } 1 < i < j < n. \tag{B-1}$$

Calling Sequence

`PBWExtension`(vars, rels, `R`, *value*)

Parameters

vars: list of variables $[x_1, \dots, x_n]$.

rels: list of relations $[rel_1, \dots, rel_t]$ determined by (B-1), where each relation rel_k has the form $[[x_i, x_j], d_1^{(ij)}, \dots, d_n^{(ij)}, d_{ij}]$ for each $i < j$.

`R`: is the coefficient ring `coeffsRing` defined as before for the skew PBW extensions.

value: boolean parameter defined as before for skew PBW extensions.

B.2. The dispin algebra.

The dispin algebra $\mathcal{U}(osp(1, 2))$ is the enveloping algebra of the Lie superalgebra $osp(1, 2)$. It is generated by x, y, z over the commutative ring K satisfying the relations

$$yz - zy = z, \quad zx + xz = y, \quad xy - yx = x.$$

Thus, $\mathcal{U}(osp(1, 2)) \cong \sigma(K)\langle x, y, z\rangle$.

Calling Sequence

`DispinAlgebra`(vars, char=p)

Parameters

vars: list of variables $[x_1, x_2, x_3]$ (the order determined by vars is $x_1 \succ x_2 \succ x_3$); this parameter is *optional*, if it is omitted then the list of variables assigned is $[x, y, z]$,

p : characteristic of ring $\boldsymbol{K}$; this parameter is *optional*, if it is omitted then the characteristic assigned is zero.

B.3. The Manin algebra of 2×2 quantum matrices

This algebra is also know as the coordinate algebra of the quantum matrix space $M_q(2)$ (cf. [54] and [63]). By definition, $\mathcal{O}_q(M_2(K))$, also denoted $\mathcal{O}(M_q(2))$, is the coordinate algebra of the quantum matrix space $M_q(2)$, it is the K-algebra generated by the variables x, y, u, v satisfying the relations

$$xu = qux, \qquad yu = q^{-1}uy, \qquad vu = uv, \tag{B-2}$$

and

$$xv = qvx, \qquad vy = qyv, \qquad yx - xy = -(q - q^{-1})uv. \tag{B-3}$$

where $q \in K - \{0\}$. Thus, $\mathcal{O}(M_q(2)) \cong \sigma(K[u])\langle x, y, v\rangle$. Due to the last relation in (B-3), we remark that it is not possible to consider $\mathcal{O}(M_q(2))$ as a skew PBW extension of K. This algebra can be generalized to n variables, $\mathcal{O}_q(M_n(K))$, and coincides with the *coordinate algebra of the quantum group* $SL_q(2)$, see [18] for more details.

Calling Sequence

`ManinAlgebra`(q, vars, char=p)

Parameters

q: parameter defined in relations (B-2) and (B-3), q must be invertible in K.

vars: list of variables $[u_1, x_1, x_2, x_3]$ (the order determined by vars is $x_1 \succ x_2 \succ x_3$; u_1 is assigned to variable u of relations (B-2) and (B-3)); this parameter is *optional*, if it is omitted then the list of variables assigned is $[u, x, y, v]$.

p : characteristic of ring; this parameter is *optional*, if it is omitted then the characteristic assigned is zero.

B.4. Woronowicz algebra

The Woronowicz algebra denoted by $\mathcal{W}_\nu(\mathfrak{sl}(2,K))$ was introduced by Woronowicz in [78] and redefined in [68] over an arbitrary field K, it is generated by x, y, z subject to the relations

$$xz - \nu^4 zx = (1+\nu^2)x, \quad xy - \nu^2 yx = \nu z, \quad zy - \nu^4 yz = (1+\nu^2)y, \tag{B-4}$$

where $\nu \in K - \{0\}$ is not a root of unity. Then $\mathcal{W}_\nu(\mathfrak{sl}(2,K)) \cong \sigma(K)\langle x, y, z\rangle$.

Calling Sequence

`WoronowiczAlgebra`(ν, vars, char=p)

Parameters

ν: parameter defined in relations (B-4).

vars: list of variables $[x_1, x_2, x_3]$ (the order determined by vars is $x_1 \succ x_2 \succ x_3$; this parameter is *optional*, if it is omitted then the list of variables assigned is $[x, y, z]$.

p : characteristic of ring; this parameter is *optional*, if it is omitted then the characteristic assigned is zero.

B.5. Heisenberg algebra

Let K be a field, the K-algebra $H_n(q)$ is generated by

$x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n$

and subject to the relations:

$$\begin{aligned} x_j x_i = x_i x_j, z_j z_i = z_i z_j, y_j y_i = y_i y_j,\ 1 \le i, j \le n, \\ z_j y_i = y_i z_j, z_j x_i = x_i z_j, y_j x_i = x_i y_j,\ i \neq j, \\ z_i y_i = q y_i z_i, z_i x_i = q^{-1} x_i z_i + y_i, y_i x_i = q x_i y_i,\ 1 \le i \le n, \end{aligned} \tag{B-5}$$

with $q \in K - \{0\}$. Note that $H_n(q)$ is not a skew PBW extension of $K[x_1, \ldots, x_n]$, however, with respect to K, $H_n(q)$ is a bijective skew PBW extension of K:

$$H_n(q) = \sigma(K)\langle x_1, \ldots, x_n; y_1, \ldots, y_n; z_1, \ldots, z_n\rangle.$$

Calling Sequence

`HeisenbergAlgebra`(n, q, char=p)

Parameters

n: parameter defined in (B-5), it must to be non negative integer.

q: parameter defined in (B-5), it must to be invertible in K.

p : characteristic of ring; this parameter is *optional*, if it is omitted then the characteristic assigned is zero.

Remark

- The variables are determined by the following order:

  $$x_1 \succ \cdots \succ x_n \succ y_1 \succ \cdots \succ y_n \succ z_1 \succ \cdots \succ z_n.$$

- To use polynomials in $H_n(q)$, the variables must be called using the sentence: `x[i]`, `y[i]` and `z[i]`.

B.6. Univariate skew polynomial ring $R[x;\sigma,\delta]$

The univariate skew polynomial ring $R[x;\sigma,\delta]$ of injective type, i.e., with σ injective, is a skew PBW extension; in this case we have $R[x;\sigma,\delta] = \sigma(R)\langle x\rangle$.

Calling Sequence

`UnivariateSkewRing`(var, sigma, delta, char=p)

Parameters

var: variable x of the ring.

sigma: injective endomorphism σ of R.

delta: σ-derivation.

p : characteristic of ring; this parameter is *optional*, if it is omitted then the characteristic assigned is zero.

B.7. Additive analogue of the Weyl algebra

Let K be a field, the K-algebra $A_n(q_1,\dots,q_n)$ is generated by $x_1,\dots,x_n,y_1,\dots,y_n$ and subject to relations:

$$\begin{aligned} x_jx_i = x_ix_j, y_jy_i = y_iy_j,\ 1 \le i,j \le n, \\ y_ix_j = x_jy_i,\ i \ne j, \\ y_ix_i = q_ix_iy_i + 1,\ 1 \le i \le n, \end{aligned} \tag{B-6}$$

where $q_i \in K - \{0\}$. We observe that $A_n(q_1,\dots,q_n)$ is isomorphic to the iterated skew polynomial ring $K[x_1,\dots,x_n][y_1;\sigma_1,\delta_1]\cdots[y_n;\sigma_n,\delta_n]$ over the commutative polynomial ring $K[x_1,\dots,x_n]$:

$$\sigma_j(y_i) := y_i, \delta_j(y_i) := 0,\ 1 \leq i < j \leq n,$$
$$\sigma_i(x_j) := x_j, \delta_i(x_j) := 0,\ i \neq j,$$
$$\sigma_i(x_i) := q_i x_i, \delta_i(x_i) := 1,\ 1 \leq i \leq n.$$

Thus, $A_n(q_1, \ldots, q_n)$ satisfies the conditions of (iii) and it is bijective; we have

$$A_n(q_1, \ldots, q_n) = \sigma(K[x_1, \ldots, x_n])\langle y_1, \ldots, y_n\rangle.$$

Calling Sequence

`AdditiveAnalogueWeylAlgebra`(n, q, char=p)

Parameters

n: parameter defined in (B-6), n must to be a non negative integer.

q: list $[q_1, \ldots, q_n]$ defined in (B-6), each q_i must to be invertible in K.

p : characteristic of ring; this parameter is *optional*, if it is omitted then the characteristic assigned is zero.

Remark

- The variables are determined by the following order:

  $x_1 \succ \cdots \succ x_n \succ y_1 \succ \cdots \succ y_n.$

- To use polynomials in $A_n(q_1, \ldots, q_n)$, the variables must to be invoked using the sentence: `x[i]` and `y[i]`.

B.8. Multiplicative analogue of the Weyl algebra

Let K be a field, the K-algebra $\mathcal{O}_n(\lambda_{ji})$ is generated by $x_1, \ldots, x_n$ and subject to relations:

$$x_j x_i = \lambda_{ji} x_i x_j,\ 1 \leq i < j \leq n, \qquad \text{(B-7)}$$

where $\lambda_{ji} \in K - \{0\}$. We note that $\mathcal{O}_n(\lambda_{ji})$ is isomorphic to the iterated skew polynomial ring $K[x_1][x_2; \sigma_2] \cdots [x_n; \sigma_n]$

$$\sigma_j(x_i) := \lambda_{ji} x_i,\ 1 \leq i < j \leq n.$$

Thus, $\mathcal{O}_n(\lambda_{ji})$ satisfies the conditions of (iii), and hence $\mathcal{O}_n(\lambda_{ji})$ is an iterated skew polynomial ring of injective type but it is not Ore of injective type. Thus,

$$\mathcal{O}_n(\lambda_{ji}) = \sigma(K[x_1])\langle x_2, \ldots, x_n\rangle.$$

Finally, observe that $\mathcal{O}_n(\lambda_{ji})$ can be viewed also as skew *PBW* extension of K, $\mathcal{O}_n(\lambda_{ji}) = \sigma(K)\langle x_1, \ldots, x_n\rangle$. Note that $\mathcal{O}_n(\lambda_{ji})$ is quasi-commutative and bijective.

Calling Sequence

`MultiplicativeAnalogueWeylAlgebra`(n, λ, char=p)

Parameters

n: parameter defined in (B-7), it must be a non negative integer.

λ: matrix (λ_{ji}) defined in (B-7), each λ_{ji} must be invertible in K.

p : characteristic of ring; this parameter is *optional*, if it is omitted then the characteristic assigned is zero.

B.9. Witten algebra

Witten's deformation of $\mathcal{U}(\mathfrak{sl}(2, K)$ was defined and studied by E. Witten introducing 7-parameter deformation of the universal enveloping algebra $\mathcal{U}(\mathfrak{sl}(2, K))$ depending on a 7-tuple of parameters $\underline{\xi} = (\xi_1, \ldots, \xi_7)$ and subject to relations

$$xz - \xi_1 zx = \xi_2 x, \quad zy - \xi_3 yz = \xi_4 y, \quad yx - \xi_5 xy = \xi_6 z^2 + \xi_7 z. \tag{B-8}$$

The resulting algebra is denoted by $W(\underline{\xi})$. In [44] it is assumed that $\xi_1\xi_3\xi_5 \neq 0$. Note that that $W(\underline{\xi}) \cong \sigma(K[x])\langle y, z\rangle$.

Calling Sequence

`WittenAlgebra`(ξ, char=p,{Str=*value*})

Parameters

ξ: list $[\xi_1, \ldots, \xi_7]$ defined in (B-8).

p : characteristic of ring; this parameter is *optional*, if it is omitted then the characteristic assigned is zero.

value: boolean parameter that declare the structure

- if *value* is *true* then the implementation checks if the structure effectively defines a skew PBW extension, in negative case returns "*Non definite Skew PBW extension*", and the structure is not defined; in affirmative case the implementation returns "*This structure represents a Skew PBW Extension.*
- if *value* is *false* the implementation allows to realize computes with this structure but this is not defined as skew PBW extension effectively.

This parameter is *optional*, if it is omitted then *value* is predefined as *true*.

B.10. σ-multivariate Ore extension

The Ore extension $A := K[x_1, \ldots, x_n; \sigma]$ introduced in the Chapter 2 with K a field and subject to relations:

$$x_i x_j = x_j x_i, \quad x_i r = \sigma(r) x_i, \; r \in K, \quad 1 \leq i, j \leq n. \tag{B-9}$$

Calling Sequence

`SigmaOreExtension`(n, σ, char=p)

Parameters

n: number of variables, this parameter must be positive integer.

σ: automorphism of K.

p : characteristic of ring; this parameter is *optional*, if it is omitted then the characteristic assigned is zero.

Remark

- The variables are determined by the order: $x_1 \succ \cdots \succ x_n$.
- To use polynomials in A, each variable x_i must be called using the sentence: `x[i]`.

Future work

- Give a constructive proof of Lemma in Remark 2.7.2.
- Give other applications of Quillen-Suslin theorem over σ-multivariate Ore extensions.
- Realize fixes to get a best efficient implementation of skew PBW extensions.
- Implement the Gröbner basis theory in Maple for right ideals and modules.
- Apply the implementation in other areas as algebraic functional systems.

Bibliography

[1] **Acosta, J. and Lezama, O.**, *Universal property of skew PBW extensions*, Algebra and Discrete Mathematics, 20 (1), 2015, 1-12.

[2] **Acosta, J.P., Chaparro, C., Lezama, O., Ojeda, I., and Venegas, C.**, *Ore and Goldie theorems for skew PBW extensions*, Asian-European J. Math., 06, 2013, 1350061 [20 pages].

[3] **Acosta, J.P., Lezama, O. and Reyes, M.A.**, *Prime ideals of skew PBW extensions*, Revista de la Unión Matemática Argentina, 56(2), 2015, 39-55.

[4] **Adams, W. and Loustaunau, P.**, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, AMS, 1994.

[5] **Anderson, F.W., Fuller, K.R** *Rings and Categories of Modules*. Springer-Verlag, New York, 1992.

[6] **Apel, J., Klaus, U.**, *FELIX a special computer algebra system for the computation in commutative and non-commutative rings and modules*, 1998.

[7] **Artamonov, V.**, *Derivations of Skew PBW-Extensions*, Commun. Math. Stat., 3(4), 2015, 449-457.

[8] **Artamonov, V.**, *Quantum polynomials*, WSPC Proceedings, 2008.

[9] **Artamonov, V.**, *Serre's quantum problem*, Russian Math. Surveys, 53(4), 1998, 657-730.

[10] **Artamonov, V.**, *On projective modules over quantum polynomials*, Journal of Mathematical Sciences, 93(2), 1999, 135-148.

[11] **Artamonov, V., Lezama, O., Fajardo, W.**, *Extended modules and Ore extensions*, Communications in Mathematics and Statistics, 4 (2), 2016, 189-202.

[12] **Artamonov, V.**, *Artamonov, V.A., General quantum polynomials.* In Algebra (Moscow, 1998), Gruyter, Berlin, 2000, 35-48.

[13] **Artamonov, V.**, *Artamonov, V.A. and Wisbauer, R., Homological properties of quantum polynomials*, Algebr. Represent. Theory, 4 (3), 2001, 219-247.

[14] **Bass, H.**, *Proyective modules over algebras*, Annals of Math. 73, 1962, 532-542.

[15] **Bell, A. and Goodearl, K.**, *Uniform rank over differential operator rings and Poincaré-Birkhoff-Witt extensons*, Pacific Journal of Mathematics, 131(1), 1988, 13-37.

[16] **Brewer, J., Costa, D.L.,**, *Projective modules over some non-noetherian polynomial rings*, J. Pure Appl. Algebra 13, 157-163. MR 80a:13009, 1978.

[17] **Bueso, J., Gómez-Torrecillas, J. and Lobillo, F.J.**, *Homological computations in PBW modules*, Algebras and Representation Theory, 4, 2001, 201-218.

[18] **Bueso, J., Gómez-Torrecillas, J. and Verschoren, A.**, *Algorithmic Methods in noncommutative Algebra: Applications to Quantum Groups*, Kluwer, 2003.

[19] **Chaparro, C.**, *Valuations of skew quantum polynomials*, Asian-European Journal of Mathematics, 8 (2), 2015.

[20] **Coutinho, S.C**, *A Primer of Algebraic D-moodules*, Cambridge University Prees, London Mathematical Society, Student Texts 33, 1995.

[21] **Estrada, S., Garcia-Rozas, J.R., Peralta, J., Sanchez-Garcia, E.** *Group convolutional codes.* Adv. Math. Commun., 2 (2008), 83-94.

[22] **Fajardo, W.**, *Módulos Extendidos y la Conjetura de Bass-Quillen*, Tesis de Maestría, Universidad Nacional de Colombia, Bogotá, 2009.

[23] **D. Forney, Jr. (1970)** *Convolutional codes I: algebraic structure*, IEEE Trans. Inform. Theory vol. IT-16, pp. 720-738, 1970.

[24] **Gallego, C.**, *Matrix computations on projective modules using noncommutative Gröbner bases*, Journal of Algebra, Number Theory: Advances and Applications, 15 (2), 2016, 101 - 139.

[25] **Gallego, C.**, *Bases de Gröbner no Conmutativas en Extensiones de Poincaré-Birkhoff-Witt*, Tesis de Maestría, Universidad Nacional de Colombia, Bogotá, 2009.

[26] **Gallego, C. and Lezama, O.**, *Gröbner bases for ideals of $\sigma - PBW$ extensions*, Communications in Algebra, 39, 2011, 50-75.

[27] **Gallego, C. and Lezama, O.**, *Projective modules and Gröbner bases for skew PBW extensions*, Dissertationes Math., 521, 2017, 1-50; DOI: 10.4064/dm747-4-2016.

[28] **Gallego, C. and Lezama, O.**, *d-Hermite rings and skew PBW extensions*, São Paulo J. Math. Sci. 10 (1), 2016, 60-72.

[29] **Gerdt, V.P., Robertz, D.**, *A Maple package for computing Groebner bases for linear recurrence relations.*, Nuclear Instruments and Methods in Physics Research Section A, 559(1):215-219, 2006.

[30] **Gluesing-Luerssen, H., Schmale, W** *On cyclic convolutional codes.* Acta Applicandae Mathematica, 82 (2004), 183-237.

[31] **Gomez-Torrecillas, J. and Lobillo, F.J, Navarro**, *Generating idempotents in ideal codes,* ACM Communications in Computer Algebra, Vol 48, No. 3, Issue 189, September 2014, ISSAC poster abstracts, pp. 113-115.

[32] **Gomez-Torrecillas, J. and Lobillo, F.J, Navarro**, *A new perspective of cyclicity in convolutional codes,* IEEE Transactions on Information Theory 62 (5) (2016), 2702-2706.

[33] **Gomez-Torrecillas, J. and Lobillo, F.J, Navarro**, *Ideal codes over separable ring extensions,* IEEE Transactions on Information Theory 63 (5) (2017), 2796-2813.

[34] **Goodearl, K. and Warfield, R. Jr.**, *An Introduction to Noncommutative Noetherian Rings*, London Mathematical Society, ST 61, 2004.

[35] **Grayson, D., Stillman, M.**, *Macaulay 2, a software system for research in algebraic geometry*, 2013.

[36] **Greuel, G.M., Levandovskyy, V., Motsak, A., Schonemann, H.**, *Plural. A Singular 3.1 Subsystem for Computations with Non-commutative Polynomial Algebras.*, Centre for Computer Algebra, TU Kaiserslautern., 2010.

[37] **Hirata, K., Sugano, K** *On semisimple extensions and separable extensions over non commutative rings*. J. Math. Soc. Japan, 18 (1966), 360-373.

[38] **Jiménez, H.**, *Bases de Gröbner módulos sobre extensiones* $\sigma - PBW$, Tesis de Maestría, Universidad Nacional de Colombia, Bogotá, 2010.

[39] **Jiménez, H. and Lezama, O.**, *Gröbner bases for modules over* $\sigma - PBW$ *extensions*, Acta Mathematica Academiae Paedagogicae Nyíregyháziensis, 32 (1), 2016, 39-66.

[40] **Kredel, H., Pesch, M.**, *MAS, modula-*2 *algebra system*, 1998.

[41] **Kunz, E.**, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, 1985.

[42] **Lam, T.Y.**, *Serre's Problem on Projective Modules*, Springer Monographs in Mathematics, Springer, 2006.

[43] **Lequain, Y. and Simis, A.**, *Projective modules over* $R[x_1, \dots, x_n]$, *R a Prüfer domain*, J. Pure Appl. Algebra, 18, 1980, 165-171.

[44] **Levandovskyy, V.**, *Non-commutatve Computer Algebra for Polynomial Algebras: Gröbner Bases, Applications and Implementation*, Doctoral Thesis, Universität Kaiserslautern, 2005.

[45] **Lezama, O., et. al.**, *Skew* PBW *extensions: Ring and Module Theoretic Properties, Matrix and Gröbner Methods, Applications*, in preparation.

[46] **Lezama, O., Gallego, C.**, *Matrix approach to noncommutative stably free modules and Hermite rings*, Algebra and Discrete Mathematics, 18 (1), 2014, 110-139.

[47] **Lezama, O. and Latorre, E.**, *Non-commutative algebraic geometry of semi-graded rings*, International Journal of Algebra and Computation, 27 (4), 2017, 361-389.

[48] **Lezama, O., Reyes, M.**, *Some homological properties of skew PBW extensions*, Communications in Algebra, 42, 2014, 1200-1230.

[49] **Lezama, O. and Venegas, H.**, *Some homological properties of skew PBW extensions arising in non-commutative algebraic geometry*, Discussiones Mathematicae-General Algebra and Applications, 37, 2017, 45-57.

[50] **Lezama, O.**, *Gröbner bases for modules over Noetherian polynomial commutative rings*, Georgian Mathematical Journal, 15, 2008, 121-137.

[51] **Lezama, O.**, *Some aplications of Gröbner bases in homological algebra*, São Paulo Journal of Mathematical Sciences, 3, 2009, 25-59.

[52] **Lezama, O.**, *Testing flatness and computing the rank of a module using syzygies*, Colloqium Mathematicum, 117, 2009, 65-79.

[53] **Lezama, O.**, *Anillos dimensionales*, Boletín de Matemáticas, 19, 1985, 194-220.

[54] **Li, H**, *Noncommutative Gröbner Bases and Filtered-Graded Transfer*, Lecture Notes in Mathematics, Vol. 1795, Springer, 2002.

[55] **Lidl, R., Niederreiter, H** *Finite Fields*. Number v. 20, part 1 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.

[56] **Lombardi, H. Quitte, C. Yengui, I.**, *Hidden constructions in abstract algebra(6): The theorem of Maroscia and Brewer*, J. Pure Appl. Algebra, 2008.

[57] **Lombardi, Ellouz, A. Yengui, I.**, *A dynamical comparison between the rings $R\langle X\rangle$ y $R[X]$*, Preprint. Algebra, 2007.

[58] **Lombardi, Yengui, I. Barhoumi, S.**, *Projective modules over polynomial rings a construtive approach*, preprint, 2006.

[59] **Lombardi, H. Quitte, C., Dimensión de Krull explícita**, preprint, 2005.

[60] **S. R. Lopez-Permouth and Steve Szabo.** *Generalized cyclic convolutional codes - convolutional codes with additional structure.*, preprint, 2009.

[61] **S. R. Lopez-Permouth and Steve Szabo.** *Convolutional codes with additional algebraic structure*, J. Pure Appl. Algebra, 217 (2013), 958-972.

[62] **Piret, P***Structure and constructions of cyclic convolutional codes*, IEEE Trans. Inform. Theory 22 (1976), 147–155.

[63] **Manin, Yu. I.**, *Quantum Groups and Noncommutative Geometry*, Les Publ. du Centre de Récherches Math., Universite de Montreal, 1988.

[64] **McConnell, J. and Robson, J.**, *Noncommutative Noetherian Rings*, Graduate Studies in Mathematics, AMS, 2001.

[65] **Reyes, A. and Suárez, H.**, *Sigma-PBW extensions of skew Armendariz rings*, Advances in Applied Clifford Algebras, 27 (4), 2017, 3197-3224; DOI 10.1007/s00006-017-0800-4.

[66] **Reyes, A. and Suárez, H.**, *A notion of compatibility for Armendariz and Baer properties over skew PBW extensions*, Revista de la Unión Matemática Argentina, Vol. 59, no. 1 (2018), 157-178.

[67] **Reyes, M. A.**, *Ring and Module Theoretic Properties of σ-PBW Extensions*, Ph.D. Thesis, Universidad Nacional de Colombia, 2013.

[68] **Rosenberg, A.L.**, *Noncommutative Algebraic Geometry and Representations of Quantized Algebras*, Mathematics and its Applications, 330 Kluwer Academic Publishers, second edition, 1995.

[69] **Ross, C.** *On the Structure of Convolutional and Cyclic Convolutional Codes.* IEEE Trans. Inform. Theory 25 (1979), 673-686.

[70] **Smarandache, R., Gluesing-Luerssen, H., and Rosenthal, J.** *Constructions of MDS convolutional codes.* Information Theory, IEEE Transactions on, 47 (2001), 2045-2049.

[71] **Stafford, J.T.**, *Weyl Algebras are stably free*, J. Algebra 48, 1977, 297-304.

[72] **Stafford, J.T.**, *Module structure of Weyl algebras*, J. London Math. Soc. 18, 1978, 429-442.

[73] **Suárez, H.**, *Kozulity for graded skew PBW extensions*, Communications in Algebra, 45 (10), 2017, 4569-4580; DOI: 10.1080/00927872.2016.1272694.

[74] **Suárez, H. and Reyes, M. A.**, *Koszulity for skew PBW extensions over fields*, JP Journal of Algebra, Number Theory and Applications, 39, 2017, 181-203.

[75] **Vasconcelos, W. Simis, A.,**, *Projective modules over $R[X]$, R a valuation ring, are free*, Notices of Amer. Math. Soc., 18, No. 5, Abstract 71T-A178, 1971.

[76] **Venegas, C.**, *Automorphisms for skew PBW extensions and skew quantum polynomial rings*, Communications in Algebra, 42 (5), 2015, 1877-1897.

[77] **P. A. Weiner.** *Multidimensional convolutional codes*, prerint, 1998.

[78] **Woronowicz, S.L.**, *Twisted $SU(2)$ group. An example of a non-commutative differential calculus*, Publ. RIMS, Kyoto Univ., 23, (1987), 117-181.

[79] **Yengui, I.**, *The Hermite ring conjecture in dimension one*, J. of Algebra, 2008.

[80] **Yengui, I.**, *Stably free modules over $R[X]$ of rank $> \dim R$ are free*, preprint, 2008.